EBOOK EXTRAS: v5.1
Downloads, Updates, Feedback



TAKE CONTROL OF

Your Online Privacy

by JOE KISSELL

$14.99

5TH EDITION

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

your data got into the hands of a party you never dreamed would have it. You can try to control the damage, but Pandora's box is already open. It's happened to millions of people, and it can happen to you too, if it hasn't already.

That's the cost of free.

I get shocked looks when I tell people that I actually *pay* for email, software, data storage, and more. Yes, I could get it for free, but in my view, the cost (in privacy) is too high.

You may be reading this book because you realize you've made a Faustian bargain and you want to extricate yourself from it before it's too late. I applaud and support that effort! Just remember: the relentless push to extract private data for free things will only escalate. It takes effort, courage, and dedication to say no to "free" things at the cost of your privacy and say yes to good old-fashioned *paying for stuff*.

Major Data Breaches Are Increasingly Common

I remember when a data breach that exposed thousands of records (email addresses, passwords, Social Security numbers, phone numbers, or other private information) was shocking, front-page news. And yet breaches several orders of magnitude larger have become commonplace. Early in 2024, there was a breach so large—over 26 billion records—that it was nicknamed the mother of all breaches. Shortly thereafter, the RockYou2024 breach revealed 10 billion unique passwords. Plus a 15-million-record breach at Trello, a leak of 70 million U.S. Social Security numbers, and many others. But each of these was barely a blip in that day's news; gigantic breaches have become that common. What's more, we all know we're powerless to prevent them. All it takes is one bad actor, or one small programming error, and even the largest collection of data from the most responsibly run institutions can become public.

Although each major data breach results in remedial action to prevent the same thing from happening again, the volume of data big companies have about each of us and the complexity of the systems they use make it inevitable that more and worse breaches lie ahead.

Hardware Bugs Pose Challenges

Software bugs that may affect your privacy are common, but at least they can be fixed with downloadable updates. But what if one of the chips in your computer or other device has an inherent flaw in its design that could lead to security problems? Chips can't simply be patched, and it may be difficult, infeasible, or even impossible to work around such issues in software. Such was the case with a flaw in Apple's M-series chips revealed in March 2024 (see Unpatchable vulnerability in Apple chip leaks secret encryption keys at Ars Technica). Sure, Apple will fix this problem at the source in *future* versions of their chips, but there's nothing to be done about the countless millions of affected products already in the wild. The previous year, privacy-leaking hardware bugs nicknamed Downfall and Inception were shown to affect Intel and AMD processors, respectively.

In these examples, there are steps Apple and Microsoft can take to mitigate the problems, and it's extremely unlikely that any given user will face any trouble from them. The problem is, issues of this sort are beyond your means or mine to guard against. For all we know, there might be some other hidden flaw in the devices we all use every day that's giving away our secrets, and we won't know until it's too late.

Big Data Is Harder to Get Away From

Many people don't realize the extent to which a handful of giant tech companies (about which I say more later, in Big Data) have their hands in your data—*even if you never deliberately use their services or visit their sites*. That's right: Amazon, Facebook, Google, Microsoft, and other companies regularly gather information about you even if you are unaware of any involvement with them.

In an epic six-part series at Gizmodo back in 2019, reporter Kashmir Hill detailed her six-week experiment to simply go about a relatively normal life but without using any services from Amazon, Apple, Facebook (now under the Meta umbrella), Google (part of Alphabet), or Microsoft. The entire story is both fascinating and infuriating, and it may lead you to form somewhat different impressions of the five companies in question. In the years since, the problem has only gotten worse; I say more about it elsewhere in this book, but see especially Learn About the Facebook Problem.

The main thing I want to point out is that thousands of other companies rely on infrastructure provided by Amazon, Google, and Microsoft for their own services. For example, Netflix and Slack use Amazon's cloud platform to provide their services. Although that does *not* mean that Amazon knows everything in your Netflix queue just because Netflix relies on Amazon's servers, it still shows how interconnected and interdependent the tech world is. And I wouldn't blame you for worrying that an as-yet-unknown bug or vulnerability in Amazon's system might have privacy implications for the many companies that rely on it.

Then there's Google. Google isn't just a search engine; they're a provider of email, document storage, videos, maps, phone service, and numerous other capabilities. (Remember: Android, Chrome, Nest, and YouTube, among many other products and sites, are all part of Google!) Forget, for the moment, the back-end Google computing tools other developers can use; what all these public-facing services have in common is Google's legendary contextual advertising—that's how Google makes money. Google didn't create these products for the public good! And the more Google services you use, the more personal data the company has about you that can be used to target ads with ever greater precision.

By most accounts, Google works hard to prevent your personal data from falling into *other* companies' hands—after all, that would be giving away the store. But will Google be able to protect your data from everyone, forever? And can you really trust Google not to be evil with your data?

On one hand, it's not in Google's best interest to alienate their users. On the other hand, Google is a giant corporation whose primary mission is to increase shareholder value, not to protect your privacy. If push came to shove, I'd have to guess Google would choose profit over kindness. And, even the best-intentioned companies sometimes experience security breaches that leak personal data.

Even if you implicitly trust Google, you should be aware of the massive amount of information most of us give Google for free—and remember that there's always a cost somewhere. You should also review the privacy settings on Google's My Account page to make sure that, to the extent permitted, you've opted out of any data collection activities you don't want to participate in (see Remove Your Info from Google).

And, of course, you shouldn't think other companies with comparable services (Microsoft, Meta, and so on) are fundamentally different. The more data any company has about you, the more power they have—and the greater the risks to your privacy at their hands.

To end on a more positive note, Apple's track record so far indicates they consider user privacy a high priority. Yes, they're a gargantuan tech company, and yes, they collect data about you as you use their services. But uniquely among the tech giants, Apple derives little revenue from advertising—their income comes mainly from sales of hardware (like iPhones and Macs) and services (such as App Stores, Apple Music, and iCloud+). In addition, Apple has the strongest privacy story of any of the big tech companies. I won't say they're perfect or even close, but I'd trust Apple to keep my data private long, *long* before I'd trust Amazon, Google, or (especially) Facebook/Meta. I say more about this later in Discover Apple-Specific Privacy Features.

Privacy Laws Are Changing

In 2018, the European Union's GDPR (General Data Protection Regulation) took effect, which occasioned all of us getting a bunch of email messages asking us to read and agree to new privacy policies, and a huge increase in warnings about websites using cookies. But behind

those surface features is a huge change in how companies that do business in Europe are required to treat their customers' privacy, as well as far greater control by EU residents in how their private data is handled. (And, because so many companies do business worldwide, it's often easier for businesses to make global changes in their sites and policies, which bring many if not all of the benefits of GDPR to customers everywhere—not just in Europe.)

Although making the changes required for GDPR compliance were onerous for a lot of businesses (I speak from personal experience here), the net result is very good for everyone. This new regulation has teeth, and some major fines have already been imposed on businesses that have violated it.

The same year, California passed the California Consumer Privacy Act of 2018, the most rigorous data privacy law in the United States to date. As with the GDPR, the existence of this law has resulted in many companies changing their privacy policies and practices nationwide or globally, because it's easier to do things the same way everywhere. Still other privacy laws have taken force (or are under consideration) in numerous other states and countries.

In general, the thrust of new laws like these is to force businesses to be more transparent with consumers about what data they collect, when and how they do so, how they use that data, and who they share it with. It also gives consumers more control over finding out what personal information companies know about them and, in some cases, removing personal data from online databases.

But laws are one thing, and actual behavior is something else. As hopeful as these new regulations may be, they haven't led to a sudden decline in data collection or sharing, a decrease in targeted advertising, or an overall improvement in customers' privacy. Those sorts of changes, on an international, national, or even institutional level, will take a long time. Baby steps.

Note: As some laws try to improve individual privacy, other laws (in the United States, the U.K., and elsewhere) are being considered that would mandate backdoors in encryption technology and/or encrypted services, usually with the intention of preventing terrorism and abuse of children. Laudable goals, but the requirements proposed to date would effectively make encryption all but useless.

What About Privacy Policies?

Almost every website and internet service has a published privacy policy (*especially* now that GDPR and other privacy laws are in effect), and I'd think twice about using a site without one. Privacy policies spell out what data the company collects (particularly personally identifiable information, or PII), how it's used, what protections are in place to safeguard it, and so on.

Privacy policies, like software licenses, are typically full of boring, inscrutable legalese. They might be good for curing insomnia, but they're not exactly page-turners. Even so, you might find it interesting and educational to read the privacy policies from a few sites you visit often. As you do, keep the following in mind:

- Although a company may be legally obligated to publish a privacy policy stating how it uses your data, it's not required to have a policy that *protects* your privacy. A privacy policy could state, "We ruthlessly collect every scrap of personally identifiable information we can find about each user and sell it to the highest bidder, with malice aforethought." So, don't mistake the *presence* of a privacy policy for a pledge of privacy.

  For example, did you know that when you use the Venmo mobile payment system to send someone cash, every transaction is, by default, *published right on the site's homepage?* It is. You can opt out, but only if you've read enough of the privacy policy to understand that this is a necessity, and you've found the switch (on Venmo's Settings > Privacy screen) to do so.

- Privacy policies sometimes contain cleverly worded loopholes—and policies could be updated without your knowledge to become less protective of your personal information.
- However strict and commendable a privacy policy may be, it is, at best, only a *policy*—not a barrier. A company may say they store your data in a secret mountain fortress protected by a dragon, but do they have a contingency plan in case a hobbit shows up with a magic ring and a bunch of dwarfs? These things happen.
- A privacy policy does not, by itself, have the force of law. If you can prove that a company violated their stated policy, you might be able to win damages in a civil lawsuit. But that can't prevent, undo, or correct a breach of privacy.

I wouldn't want to do business with a company whose privacy policy admitted to practices I disagree with, and I'd rather know about such things up front. But even a fantastic privacy policy is no guarantee.

Note: There may be other benefits to reading the fine print carefully. A travel insurance company buried language in their policy stating that the first person to read that paragraph and email the company would win $10,000. A teacher from Atlanta claimed the prize. The insurance company hoped the publicity would encourage more people to read their policies!

Your Own Privacy Is Only Part of the Problem

It's easy to fall into the trap of thinking of online privacy as a personal thing, as though your privacy is entirely dependent upon what you do or don't do. In fact, nothing could be further from the truth. A huge part of the challenge of online privacy is that for any information transmitted over the internet, at least two parties have access.

If you send me an email or text message, we each have a copy—and our service providers probably do too. If you fill out a form on the web, you

and the company running the server both have the information you entered—and so do any third-party cloud providers, backup operators, or service operators the company uses. If you share a file with me, we both have a copy. And so on. No matter how carefully you control your own copy of such data—for example, making sure every copy of a file (including backups) is safely encrypted—you can never control what the other party does with your data.

Likewise, you're responsible not only for your own private data but also for the private data of your contacts. Even if you don't care about personal consequences from having someone observe, hack into, or steal your data, there could be severe consequences for other people. The contents of your address book, email, calendar, and so on may contain personal data about your friends, family, and coworkers that could damage them if it got out—and even if they themselves are strict about safeguarding their own data. There's also the matter, as I mentioned in Things You Might Want to Keep Private, of sharing your genetic data with DNA testing services, in that the information you provide can also reveal a lot about your relatives—for better or worse.

There are some partial exceptions to this rule, such as messaging services that delete all traces of a message from both parties' devices as soon as it's delivered. (Cue *Mission:Impossible* soundtrack!) With effort, it's possible to increase the odds that certain types of data will remain private even once conveyed to another person—as long as the other party doesn't speak, write down, or take a screenshot of what you said. But for most types of data, and most situations, that's not feasible.

Although this may seem a depressing state of affairs, I call your attention to it in the hope that it'll encourage you to be more thoughtful about what information you share online and how you protect the information others have shared with you.

See How Bad Things Are

This is going to hurt, and you're not going to like it at all. But for your own good, I suggest doing a mini privacy audit of yourself, just to get an approximate sense of how things stand today. I'm not talking about anything formal or detailed, just something like this:

- **Google yourself.** Yes, use Google, not a more-private search engine, because the point of the exercise is to see what the world's biggest search engine knows about you. Page through the first few hundred results and see what you find.
- **Check for leaked credentials.** Go to Have I Been Pwned?, enter your email address, and see if that address has appeared in any major data breaches. Do you have several addresses? Repeat the search with each of them. Every hit means a password of yours that the bad guys might know.

Note: 1Password's built-in Watchtower feature can automatically check your email address(es) against the Have I Been Pwned? database to see if any of your passwords are potentially compromised and in need of changing.

- **Search for yourself at a data broker or two.** Pick a data broker (see Purge Your Info from Data Brokers). Enter your name and other pertinent information and do a search. See what data they already have about you—and remember, any or all of it may be wrong! (Keep in mind that most data brokers want you to *pay* them to see all the personal information they have about you! I don't recommend paying them, but even seeing what they show you for free can be quite eye-opening.)

If you're like most people, you'll be unhappy about what you find in these searches. You may find true facts that you didn't think anyone else would know, as well as blatant errors. You might find out that people have said some extremely unkind things about you. You might find that a simple (or even embarrassing) password of yours is public knowledge.

I don't want you to be unhappy, but I do want you to have some real-world information to help guide your decisions. With this data in hand, spend some time reflecting on how willing you are to continue giving up privacy (or your friends' privacy) for free stuff. If you feel motivated to take action—and I hope you do—you can start right away. That's what the rest of this book will help you to do.

Is It Too Late to Protect Your Privacy?

I was chatting with some family members who described how they were freely sharing a truly disturbing range of information with the likes of Amazon, Facebook, and Google. I briefly explained why that was kind of not great from a privacy perspective, and…let's just say that put a damper on what had been a pretty cheery discussion. (Uncle Joe. What a buzzkill!)

Then my niece, who seemed particularly troubled by my revelations, asked a really great question: "OK, I get that this is bad. But if I've already been sharing all this data with these companies for years, is there any point in changing what I do now? They already have the data, so isn't it too late?"

I said, "Think about it this way. You can't un-murder someone, but it's never too late to stop murdering more people." And yes, I know, that was kind of overdramatic. But my point was, even if you've revealed things about yourself that you shouldn't have, it's still a *great* idea to stop revealing more! (And, as I explain throughout this book, you can take steps to remove at least some of that private data you've already given away.)

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?

- **Financial information:** You may file your taxes online, and you may submit online applications for credit or other financial services. That's all fine; tax authorities, banks, and lenders have a legitimate need to know how much money you earn, what your Social Security number is, and so forth. But I'll bet you wouldn't want *everyone* to know that information. Likewise, you can probably log in to your bank accounts online, but it may not be in your best interest for just anyone to see your bank statements. And yet, any information that's transmitted online could conceivably be misused.
- **Medical information:** Everything that your doctor knows about you—your height and weight, past and present illnesses, surgeries, medications, pregnancies, genetic data, and so on—is almost certainly stored in a computer somewhere. If a security breach or human error resulted in any of that information leaking, or if you shared it injudiciously by email or social networking, might that have any negative consequences? The same goes for genetic information about yourself (and your relatives) stored online if you've used a DNA testing service such as 23andMe or AncestryDNA.
- **Purchases:** When you buy anything online, the vendor keeps a record. Your bank knows about all your transactions, too, if they were with a credit or debit card. Some of your purchases will also be known to online advertisers. All that data is online somewhere—and some pieces of it are more secure than others. Can you think of any purchase or transaction you might not want to be made public?
- **Communication history:** Some of us deliberately save every email message we receive or send, but even if you don't, that information (possibly including messages you deleted long ago) is out there—it's on a server somewhere, or on someone else's computer. Ditto for text messages, chats, forum posts, comments, and most other forms of electronic communication. Most of it is probably innocuous, but if you ever sent a message that you wouldn't want your mother, spouse, or employer to read, you may have a legitimate worry about your online privacy.
- **Browsing behavior:** You're aware, I'm sure, that every website you visit, every web search, every video you watch, and every file

you download leaves a trail, which includes information about your location, your computer, and your browser, among other things. Parts of this trail are stored on your own computer or mobile devices as histories, caches, and cookies. Some parts are stored on the servers of search providers, advertisers, and other entities. It's extremely difficult to avoid leaving a trail and virtually impossible to erase all traces of your browsing behavior after the fact.

I could go on, but I hope I've made my point. You want your real-life friends and family to know where you are and what your kids are doing; you don't want strangers to know. You want to order things online, but you don't want your spouse to know about the surprise birthday present you bought. You want your sister to know you're pregnant, but you want to wait before letting your parents or your employer know.

Unfortunately, you can't always control what happens to information about yourself on the internet. Far too often, for one reason or another, online information about you becomes available to people or organizations that you would prefer didn't know it—and this usually happens without your knowledge.

Personally Identifiable Information

In the foregoing list, I assumed all the information about yourself that could conceivably "escape" online can be traced back to you. Sometimes that's true, but not always.

If you read the privacy policies of the websites you visit (an admittedly boring undertaking that I discuss further in What About Privacy Policies?), you'll notice that they normally distinguish between *personally identifiable information* and *anonymous* or *aggregate* information. This difference is worth understanding.

If a message, database entry, or other snippet of information online includes your full name, your email address, your photograph, your driver's license number, or some other detail that uniquely belongs to you, it's personally identifiable—even if the person or company who has that information hasn't actually identified you with it.

On the other hand, some information—your city, area code, operating system, and so on—is the same for many people. An advertiser may find it useful to know that 145 people in Fresno who also own iPhones visited a certain webpage today, but if you were one of them and that's the only information the advertiser has, it won't point to you personally. This sort of aggregate demographic information is valuable to businesses, political campaigns, and other entities even it doesn't identify you personally. But sometimes a combination of seemingly innocuous facts can turn aggregate information into personal identification (I explain how in On a Web Server).

IP addresses are an interesting case. Every device that connects to the internet uses one, although often more than one device shares an IP address (often using a technology called NAT, or Network Address Translation), and a device's address may change from time to time. When you visit a website, it records your current IP address. If you happen to be using a device whose IP address isn't shared, that number can potentially be traced back to you personally. But if you visit the same page at, say, a public library or using a device connected to a public Wi-Fi hotspot, the IP address recorded by the website would not be personally identifiable.

Privacy vs. Security vs. Anonymity

The words privacy and security are often tossed around as though they're synonymous, and some people also confuse privacy with anonymity. In fact, these three words all mean different things, but the concepts are related, especially when it comes to the internet:

- **Privacy** is freedom from observation or attention.
- **Security** is freedom from danger or harm.
- **Anonymity** is freedom from identification or recognition.

To picture the difference between privacy and security, think of a bear. When you visit a bear in a zoo, you have no privacy (anyone can see you) but you have near-total security in regard to the bear: it's very unlikely the bear will harm you. On the other hand, if you're in a tent in the woods, you might have privacy (no one can see you) but not security (a bear could slash right through your tent and harm you). Either way, you're anonymous from the bear's point of view (it doesn't know you), but once your remains are identified, we'll know who you were.

Bears tend not to use the internet, but you might have **privacy** online if no one can see what you type, the contents of your email, which sites you visit, and so on without your permission. If you are safe from malware, hackers, and other potential causes of harm (including data theft), that's **security**. And if you send a message or visit a website without anyone being able to tell that it was you in particular who did so, that's **anonymity**.

Computer security can often increase your privacy, just as a lock on your door (security) can prevent someone from opening it and seeing you in your underwear (privacy). But there are situations in which you might have privacy without security, and vice versa.

Likewise, if I send you a message only the two of us can read, it's private—but not anonymous if we know each other's identity. If I post a comment anonymously on a website, it's not private at all, even though no one may know who it's from.

Learn Who Wants Your Private Data (and Why)

We've seen that lots of information you may want to keep private travels over the internet. That in itself isn't a problem; after all, you *want* to share private information with your family, friends, doctor, and so on. Problems can occur when someone accesses personally identifiable information without your consent or even, in some cases, your knowledge.

Who exactly might be trying to learn private information about you online? I'm glad you asked; here I show you who wants to know about you and, crucially, *why*. Knowing who you're trying to keep your private data private *from* is a useful first step.

Advertisers—and Beyond

The internet is powered by advertising as much as it's powered by servers and routers. Many websites devote far more space and resources to ads than to their actual content. As you know, it's difficult to read the news, watch a video, check your email, or even search for pictures of cute cats without being bombarded by ads.

Websites sell advertising space because they can't come up with any better ways to make money. And, of course, it's not just the web. Ads show up in apps on all your devices, on your smart TV, in podcasts, and anywhere else someone thinks they can make money with them.

The companies that purchase advertising want to get their money's worth, and that happens only if the ads result in sales. So advertisers expend a tremendous amount of effort to ensure the ads each person sees are likely to be interesting and relevant, and thus lead to purchases. When advertisers make money, they're able to keep buying ads and the companies that display the ads in their apps on their websites can keep making money too.

Years of experimentation have shown that the most effective ads are those that target *individual* needs and preferences—including things

you didn't even think you needed! For example, if an advertiser knows I'm in the market for an air conditioner and shows me an ad for one—even on a completely unrelated site—the chances of making a sale go way up compared to generalized ads merely relevant to a site's content or the perceived needs of a broad demographic group.

How might an advertiser know I'm in the market for an air conditioner if I'm not on a site that sells air conditioners? There are a number of techniques, including tracking cookies (see Manage Local Storage of Private Data), but most involve storing hidden data on my device (or profiling unique or nearly unique aspects of my device) when I visit one site (say, a search at Amazon.com) and then checking that same data when I go to another site (say, weather.com) that displays an ad from the same provider or advertising network. Although the server may store the details of my visit, my device profile and/or the data stored locally on my device enable advertisers to identify me across sites.

Note: Amazon and Google are special cases because they're wildly popular, act as both vendors and as platforms for other vendors, and sell devices that can listen to everything you say. Further, Amazon's affiliate program can make their Amazon ads pervasive. (Why pay for advertising when millions of people will do it for you in exchange for a trivial referral fees on purchases?) Amazon and Google are also notoriously chatty with your devices.

As you search the web, browse various sites, follow links, and use ad-supported apps, advertisers compile elaborate profiles of your perceived interests and tastes. And, because your IP address (or profile information you've entered into a service like WhatsApp or Facebook) tells them roughly where you are, they can even display ads for local businesses selling the products you've shown interest in.

In fact, I'm downplaying the scope of the problem by making it sounds as though you're tracked only when you deliberately take some action. Merely having your phone in your pocket or having a smart speaker in your home can result in an astonishing amount of passive data collection. (Joan Is Awful, an episode of the Netflix series *Black Mirror,*

takes this concept of passive tracking being used against someone to an extreme, but I found it somewhat uncomfortable because it's only barely fictional: nearly everything in that episode is at least theoretically possible with today's technology.)

From the perspective of the advertisers and the companies that rely on advertising for income, this is supposed to be good news, because it means the ads you see and hear—they take for granted, of course, that you'll constantly be seeing and hearing ads—are more relevant to you than if they weren't targeted. Isn't that nice for you?

But…

Individually targeted advertising isn't always to your benefit. The same bits of data that advertisers can piece together to determine your interests and location can be used for things like showing higher prices on furniture to people who live in wealthy neighborhoods—or higher prices on electronics to people using Macs rather than PCs. (Yes, these things actually do happen.) They could also be used to determine that you are a registered voter in the "wrong" party, resulting in a phone call or text message sending you to the wrong polling place.

In fact, the privacy concerns get even worse. Imagine this scenario, only slightly fictionalized from real life. A retailer tracks your online purchases and, noticing that you're buying larger clothes, folic acid, and unscented lotions, guesses that you might be pregnant. Then, in an effort to be "helpful," they display ads for baby clothes and cribs—or maybe they even send such ads by mail. Now family members, coworkers, or other people who might see those ads *also* suspect that you're pregnant. Oops. (It gets even worse if a pregnancy goes wrong.)

The variations on this theme are endless, but the point is that advertising can never be targeted with perfect precision. Advertisers may think they're showing ads only to you, but your spouse, parents, kids, or anyone else who might use the same accounts or electronic devices can also infer private information about you by seeing on your screens the ads that were targeted at you.

Beyond the fact that merely showing you targeted ads can cause problems, the deeper and more insidious danger comes from the tracking techniques used to learn all about you, and the secret profiles about you that advertisers have at their disposal. Over time, the methods used to track you have become increasingly sneaky and sinister, the data collected has become more detailed and personal, and the uses to which that data has been put have gone way beyond showing ads. Because—surprise!—advertisers aren't the only ones who use that data. So do credit agencies, employers, insurance companies, law enforcement agencies, and governments, among others. Misuse of profiles gathered in this way has led to lost jobs, failed relationships, and far worse. The ads themselves are a problem, but they're only the tip of the iceberg. The underlying tracking has become the real issue, and however creepy you might already think it is, the true scope of the problem is almost certainly worse.

We can stop pretending that tracking and profiling you is in any way honorable. It's not for your benefit; it's for the benefit of people making money from you. So, quite a lot of this book discusses ways to curtail this tracking and limit its use.

Privacy and Your ISP

So far, I've largely pretended that the records of what you do on the internet are stored only on your devices and on the servers belonging to sites you visit. That's an oversimplification. In particular, ISPs—the companies that provide your connections to the internet, whether broadband, cellular, satellite, or dial-up—can and probably do log every connection between your devices and other devices elsewhere on the internet. It's comforting to think of ISPs as being mere conduits for information, but in fact your ISP can tell exactly where you go on the internet, when you do it, and (in many cases) what you're doing.

ISPs can use this data for legitimate reasons, of course, including troubleshooting and performance optimization, detecting and preventing abuse, enforcing the company's terms of service, and so on. Your ISP may also provide this data to law enforcement or government agencies if legally obligated to do so.

However, this data has a more disturbing use, too. A law in the United States passed in 2017 explicitly allowed ISPs to sell browsing and usage data to marketers *without customers' consent or knowledge*, and prevented the Federal Communications Commission from making rules that would disallow this behavior. The upshot is that there are even more ways your private data can be handed to advertisers, and more ways ads can be inserted into your internet use. (For details, see the EFF's articles Repealing Broadband Privacy Rules, Congress Sides with the Cable and Telephone Industry and Five Creepy Things Your ISP Could Do if Congress Repeals the FCC's Privacy Protections.) In 2024, the FCC once again reclassified ISPs as common carriers which, in theory, reinstated protections on sharing or selling identifiable customer data. However, the broadband industry is widely expected to fight these changes in court.

The fact that ISPs have been *allowed* to do this does not automatically mean they do. All the same, I suggest checking your ISP's privacy policy and terms of service to see their current stance.

You have other options, too. For example, virtual private networks (VPNs) can often hide your browsing behavior from your ISP (see Use a VPN).

Data Brokers

You may have the impression that each advertiser or ad network is trying to profit directly from your data, but that isn't necessarily the case. Sometimes tracking data is used primarily to display ads on the spot, but those personal profiles created by tracking your online behavior can be sold for a profit.

A *data broker* is a company that tracks your information in order to sell it—to advertisers, government agencies, or pretty much anyone who's willing to pay (including Doxxers). Some advertisers are also data brokers: they use your information themselves and also profit by selling it to others.

To learn more about data brokers and the astonishing amount of information they have, see:

- Data broker at Wikipedia
- Data Brokers and Personal Data Deletion Services: What You Should Know at CNET
- Everything you need to know about data brokers at OpenMedia

I talk about removing your personal data from such companies later, in Purge Your Info from Data Brokers.

Everyone Else

Although advertisers and data brokers are, in my opinion, the biggest and most worrisome threats to your online privacy, there are many other people and groups who might want your personal data. Here's a partial, incomplete list.

Local Villains

One category of people who might be out to get the digital goods on you is what I'll call "local villains." Let me give you some examples:

- Ex-spouses or former partners who want to make your life miserable or even find evidence to use against you in court

- Your current employer, who may want to make sure you're not violating company policies or misusing proprietary information
- A prospective employer who's trying to judge your appropriateness for a position
- Stalkers, thieves, and other criminals looking for evidence of when you're home or not, where your kids are, and other information

As a group, local villains tend to be less technologically sophisticated than advertisers, hackers, and others who seek your personal information. On the other hand, they may be more motivated, and they're far more likely to be focused on you *personally* rather than on a sales demographic you represent. And, let's face it, most of us have tons of personal information online that's readily accessible by the general public—Facebook, Instagram, personal blogs, and so on.

Doxxers

Doxxing (derived from the word "documents" and sometimes spelled *doxing*) is the act of discovering and publishing private information about someone else—for example, the real-life identity of someone who uses an alias on the internet, or a person's home address or private phone number. Although doxxing can sometimes be used for good (say, unmasking a criminal), it's most commonly used as a tool to harass and threaten someone the doxxer dislikes.

Note: Taken to an extreme, doxxing can become *swatting*, in which someone reports a serious crime at your location, resulting in a raid by a SWAT team (or other heavy-duty law enforcement).

Although anyone could be doxxed (and it does sometimes happen for ridiculously trivial reasons), those at greatest risk include celebrities, activists, and anyone who supports, promotes, or comes to be identified with a controversial cause. And, sorry to say, women—especially those who work in the tech industry—are at much greater risk for doxxing than men.

Because many doxxers rely on information compiled by Data Brokers, you can decrease your risk by removing your data from brokers that

allow you to do so—some do, some don't. I say more about this in Purge Your Info from Data Brokers.

Hackers

Some of them do it for fun. Some do it for notoriety. Some do it to make money. But one way or another, thousands of intelligent but misguided people around the world spend most of their waking hours trying to break into computer systems to steal information and money, to trick you into buying something, or simply to cause mischief.

I shouldn't call them "hackers," because hacking is a noble art and only a small subset of hackers use their powers for evil. But you know what I mean: black hats. People—mostly young men—who write and distribute viruses, keyloggers, Trojan horses, ransomware, and other malware. People who send spam and use phishing messages to con you into handing over your passwords. People who take over computers by the millions to turn them into botnets. Bad guys.

Hackers rarely target specific individuals—in most cases, it's nothing personal. The two pieces of private information most of these bad guys would be happiest to have are your credit card number (for obvious reasons) and any password that protects financial information (for the same reasons) or provides access to large amounts of your data, such as your email account. Although it's difficult to protect your privacy from a truly determined hacker, you can take steps (as discussed elsewhere in this book) to make their work harder and less rewarding.

Note: If you want to see what the bad guys—hackers and others—have been up to lately, you can search in the massive (although incomplete) database of the Privacy Rights Clearinghouse for privacy breaches. It's fascinating and deeply sobering: the list is enormous and growing constantly.

Big Media

The RIAA (Recording Industry Association of America) and MPAA (Motion Picture Association of America)—along with record labels, movie studios, publishers, game developers, and other major copyright holders—are keen to know who has been pirating their media. Apart

from monitoring popular services (like YouTube, Twitch and Discord), BitTorrent traffic, and file sharing sites, these firms work closely with ISPs to identify people who illegally share movies, television shows, music, games, software, and other copyrighted materials. Depending on your location and provider, this could lead to serious consequences including civil lawsuits and termination of your internet service.

I don't blame copyright holders for protecting their property; I've had my own work pirated and lost money because of it, and it's no fun. (You *did* pay for this book, right? Just checking. If not, I should mention in passing that I can see you right now.)

The problem is, sometimes big media companies make mistakes. They've sued little old grandmothers who don't even own computers and made other egregious blunders. Even if you'd never consider stealing media (I did tell you I'm watching, right?), you might prefer that your downloading and streaming activities be kept private.

Big Money

Banks, credit unions, credit card providers, and other financial institutions may want evidence of your thriftiness or trustworthiness in considering whether to offer you a mortgage or other loan. Insurers may want to see whether you engage in risky behavior or have medical conditions that might influence your rates or disqualify you. When lots of money is at stake, it's only prudent to collect as much information as possible to make a good decision. That's as true for large corporations as it is for you.

You should not be at all surprised if a potential lender or insurer checks out your Facebook page or searches for your name on Google. Your health-food blog and tweets about your jogging regimen might score you a better life-insurance premium; Facebook posts about late-night drinking binges could raise your car insurance rates. You may never learn *why* these things happened, either—companies generally aren't required to reveal how they go about researching you.

Big Data

I've mentioned Google (and will do so again)—it's one of the largest non-governmental data collection entities in the world. But it's certainly not the only one. Facebook, Microsoft, Amazon, X (formerly Twitter), and other companies with users numbering in the hundreds of millions (or more) collect massive amounts of data on users' tastes, opinions, geographical whereabouts, and other details—including physical appearance and biometric information. Although this data is mostly used for targeting advertising (see Advertisers—and Beyond), it can also be put to many other uses, from the virtuous (helping you find a parking space) to the creepy (profiling you as a potential criminal).

Big Brother

A string of revelations published widely starting in mid-2013 detailed ways in which government agencies, including the NSA (National Security Agency) in the United States and Britain's GCHQ (Government Communications Headquarters), have been secretly collecting phone records, email, text messages, recordings of Skype conversations, and other data most of us thought was private—on the authority of secret courts and accompanied by gag orders that prevented those who knew about the data collection from revealing it. In fact, this sort of thing has been going on for a long time, and there's no end in sight. The public might never know the full nature or extent of government data monitoring.

Tip: For detailed and continuously updated discussions of the ongoing revelations about government monitoring, see 2010s global surveillance disclosures at Wikipedia.

All this is being done, of course, in the name of preventing terrorism and other crimes. You may or may not believe that. You may trust your government and feel that a reduction of privacy is justified by an increase in security, or you may feel the whole thing is an appalling abuse of power. Whatever your opinions, I believe the following facts are uncontroversial:

- Massive data collection has happened and continues to happen. There are apparently no *technological* barriers preventing the

government from monitoring most email, phone calls, and other online data.

- The laws governing data collection may eventually change, but if the monitoring by the U.S., UK, and other governments was performed for years without the public's knowledge that the law permitted it, the same thing can happen again. (And in any case, making something illegal doesn't mean it won't occur.)
- Although we now know something about data collection by the NSA, FBI, and other U.S. law enforcement agencies, and comparable efforts in certain other countries, the full extent of global monitoring is unknown. It's plausible that other governments have the capability to capture at least some of your personal data, even if you access internet services only in your own country.
- Other than lobbying for changes in laws you may disagree with and voting for people whose privacy positions you trust, there's little that average citizens can do about this sort of data collection.

Going back to the "I have nothing to hide" argument (see Learn What You Have to Hide), the difficulty with all this from a privacy point of view is that even if you are the most harmless and trustworthy person in the world, something you say or do online could be misconstrued or misrepresented. Just as spam filters incorrectly flag some legitimate messages as junk mail, government computers could incorrectly flag you as a potential threat, and that could have consequences ranging from inconvenient (such as being put on a no-fly list) to devastating (being charged with a crime you didn't commit). Computer programs have been known to make mistakes—and so have the people using them.

In fairness, government agencies also collect massive amounts of data for much more mundane reasons—think of the Centers for Disease Control, the Census Bureau, the Social Security Administration, and the Internal Revenue Service, for example—making them another variety of "big data." Even so, the problem remains that you have no idea who might access or use your information, or for what purpose.

I should also mention in passing that it's not just the *current* government that wants to know all about you. Political parties—and candidates running for future office—are also keen to know everything they can, in order to target ads and perhaps sway your vote. And guess who else has an interest in how your country's elections turn out?

Foreign Governments

Assuming you've at least glanced at the news once or twice in the past decade, you're surely aware that several nations' governments—most notably those of Russia, Iran, China, and North Korea—have been implicated in using the internet (especially Facebook and X) to influence elections in other countries, sow discontent and discord, and distract people from human rights abuses. Much of this activity has been precisely targeted using exactly the same private data and unscrupulous methods as online advertisers, often in combination with sophisticated fraud, hacking, and captured/fake accounts set up to deliberately spread misinformation.

These regimes and others also operate and/or sponsor ransomware and extortion operations targeting individuals, businesses, schools, hospitals, and public infrastructure. In many cases (particularly against individuals) the attacks are carried out using private data gleaned from data breaches and other online sources.

Your Risk Profile

I had an aunt who lived alone and was terrified that someone might break into her house, even though she owned nothing of any value whatsoever. So she put about half a dozen separate locks on her front door, which made it tedious for her to open it when a family member came to visit—and would have been a serious risk to her safety if there had been a fire or medical emergency. Her actions were out of proportion to the risk she faced, and ironically they made her less safe.

When it comes to your online privacy, there's also a relationship between how tightly you lock down your information and how inconvenient your own life becomes. The amount of effort you put into protect-

ing your privacy, and the amount of aggravation you must endure, should be roughly proportional to what's at stake.

You don't need to perform an actuarial calculation to determine where you fall on the risk spectrum. But you should give a bit of thought to what is, and is not, worth worrying about in your situation.

Generic vs. Targeted Threats

When advertisers use algorithms to show you ads for things that align with their profiles of you, you may *feel* as though you're being individually targeted, but it's not really about you specifically; it's just your data matching up with what someone is selling, and the same would be true of anyone else who went to the same sites and did the same things online. Most of the threats to your online privacy are, in fact, in this "generic" category. Yes, your personal information is being used—and yes, it may affect you in a negative way—but it's all done automatically, by computers, without any consideration of who you are.

By contrast, if you're a millionaire, a celebrity, a politician, a witness to a crime, or someone with a valuable secret, you could be targeted as an individual. They want your money, your political cooperation, your secret, or whatever. Similarly, if you've made an enemy for whatever reason, that person may want to cause you harm. In cases like these (see Cope with Special Cases in the next chapter), where you are or potentially could be targeted personally, much more is at stake, so more elaborate privacy measures are warranted.

Other Risk Factors

Someone recently told me they have never typed their credit card number into a computer. They had a mistaken idea about the risk of doing so, which is extraordinarily small. Credit cards already come with protection against fraudulent use, and hundreds of millions of people safely make credit card purchases online everyday. The risk isn't *zero*, but it's not worth worrying about, for most people, as long as you exercise reasonable discretion.

I'd like you to think about risk—in other words, what you should or should not worry about—in a different way. It's all about context. For example:

- **Type of device:** All things being equal, laptops are more vulnerable than desktops, because they're easier to steal (or lose), and more likely to be out of your physical control. Mobile devices (smartphones and tablets) are even more vulnerable to theft, but they're also more likely than laptops to be locked, by default, with a passcode or biometrics, which may make their *data* generally less vulnerable.
- **Location:** If you're at home, with the doors locked, your devices and their data are at a much lower risk than if you're using them in a coffee shop or other public place—especially if it's an environment where someone might be able to "shoulder surf" as you type passwords and passcodes.
- **Profession:** People in fields like law, medicine, finance, politics, and (in some cases) technology may have personal data that's perceived to be worth stealing. If you're a retail employee, teacher, or construction worker, for example, your profession by itself is unlikely to make you a target.
- **Lifestyle:** If you spend a lot of time in bars and at parties, mingling with strangers and surrounding yourself with loud music, alcohol, and drugs, well, you're probably going to be more vulnerable to a privacy incursion than if your idea of a good time is hanging out with the other monks at the monastery, meditating and praying for peace.

All that to say: most of us—ordinary folk who aren't protecting vast fortunes or state secrets—have an average risk level. A retired teacher who lives alone in a rural cabin and uses a desktop computer mainly for playing chess online has a super-low risk level. Taylor Swift, Tim Cook, or Prince Harry would be at the other extreme, in need of the strongest possible privacy measures.

Additional Resources for High-Risk People

I'm going to make the bold assumption that the vast majority of people reading this book are in the low-to-average risk category. So most of what I recommend is based on ordinary privacy needs. However, if you do find yourself in a higher-risk category (see Cope with Special Cases, in the next chapter), I have some extra help for you. Throughout the book I've sprinkled a series of "High-Risk Resources" sidebars that offer advice for cranking up your privacy (even at the cost of convenience) when the need arises.

What You Can't Control

No matter how careful you are, how tightly you lock down your privacy settings, and how many hoops you jump through with tools like ad blockers, VPNs, and encryption, there will always be privacy risks you couldn't predict or plan for. You can do all the right things—even all the *extreme* things—and still suffer a privacy breach. Some of the things you can't control are:

- **Changing privacy settings:** Companies like Facebook, Google, ISPs, and cellular carriers that collect a lot of data about you have a vested interest in preventing you from changing any settings that might interfere with that. You shouldn't be at all surprised to see that privacy settings have moved or disappeared, or that you've been opted in for some new type of data collection without notification or consent to "improve your experience."
- **Security breaches:** Your private data—even if you offered it voluntarily and even if it was encrypted and subject to the most strenuous privacy laws—could still get out and cause you grief (refer back to Major Data Breaches Are Increasingly Common).
- **Hardware and software bugs:** Flaws in apps, operating systems, and even chips can also lead to disclosure of data that you had every reason to believe was private.
- **Tech companies adopting unscrupulous technologies:** Because of the vast fortunes to be made from advertising (and other-

wise exploiting personal data), tech companies are constantly developing new ways to collect data about you and prevent you from stopping it (or even, in some cases, even knowing about it).

I can't make you feel better about all this, except to use my best Robin Williams impersonation and say "It's not your fault," over and over. But I do want you to be aware of the limits to the solutions anyone can give you for keeping your data private.

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

collect lots of data about you. And switching mobile platforms could be an expensive and frustrating experience.

- **Install a good ad blocker:** Even if you don't care about seeing ads, as such, ads can help companies track what you do merely by showing up on a screen (see Block Ads). Because you want to reduce the amount of personal data collected about you as much as possible, preventing ads from appearing at all produces huge privacy benefits.

  BUT: There are no perfect ad blockers (though some are quite good). Some sites won't work properly when an ad blocker is enabled. And some devices that display ads, like smart TVs and streaming devices, have no capability to run ad blockers, meaning you'd have to depend on a separate, network-wide device (see Consider a VPN Router or Privacy Appliance).

- **Encrypt everything:** Instead of plain SMS, use an encrypted messaging system such as iMessage or Signal (see Talk and Chat Privately). Switch to an encrypted email provider (see Encrypt Your Email). Use encrypted Wi-Fi connections when possible. Use a VPN to encrypt your internet connection (see Use a VPN). Basically, wherever there's an option to encrypt communication, take it!

  BUT: Encryption isn't a perfect or complete solution, and often, encryption introduces compatibility problems that require work and cooperation from all the parties that are communicating. Sometimes it costs extra, too.

- **Just say no:** Whenever a website, app, device, or service asks you for permission to do anything that affects your privacy (like your location), say no, enabling only the very specific services you truly need. Opt out of third-party cookies on every website. Change all your privacy settings to make it as hard as possible for other people to discover your personal information

  BUT: Golly, that's a lot of work. And tech companies sometimes deliberately design things so that they won't work correctly unless you enable intrusive features.

So, even though I wish it were that simple, realistically, it's more complicated and involved.

Choosing Better Passwords

In my book *Take Control of Your Passwords* I go into great detail about what makes passwords better or worse, why so many people choose bad passwords so much of the time, what problems bad passwords can cause, and how to create great passwords without going crazy. For our current purposes, however, I want to point out that using bad passwords *massively* increases your risk of having private data exposed. Although great passwords don't give you an ironclad guarantee of privacy, they do put a significant barrier in the path of a prospective attacker, and they're one of the easiest steps you can take to protect your privacy.

Here's a brief summary of my password advice:

- **Never reuse passwords.** Every site, service, and account should have a unique password, so that if one is compromised, the damage will be contained.
- **Go long, random, and diverse:** Mathematically speaking, the strongest passwords—those most resistant to guessing even by powerful computers—are long (15+ characters), randomly generated, and composed of a combination of upper- and lowercase letters, digits, and punctuation.
- **Use a password manager:** It's hard for a human to come up with a sufficiently long and random password, and even harder to remember such a password (especially if you have dozens or hundreds of different ones). A password manager app (such as 1Password or Bitwarden) can generate, remember, and fill in strong passwords for you, and securely sync them across your browsers, computers, and mobile devices. I say more about these in Protect Passwords and Credit Card Info.

About Two-Factor Authentication

Two-factor authentication is when a site or service needs more than your username and password—it also needs another *factor*, which could be a physical token, a fingerprint scan, or any of numerous other options.

A variation on this theme, sometimes called *two-step verification,* typically requires you to enter a numeric code sent as a text message to your mobile phone or generated using a mobile or smartwatch app such as Google Authenticator, Authy, or 1Password. (Authy now offers a simplified approach, in which you need only tap a button on a paired phone or Apple Watch.) Because these codes change frequently—typically every 30 seconds to 5 minutes—they're effectively immune to many types of theft and guessing that could compromise an ordinary password. However, don't think of SMS and authenticator apps as being equivalent in security! Given the choice, you should always avoid SMS for authentication, because SMS is too easy to hack.

Apple, Dropbox, Evernote, Facebook, Google, PayPal, X, and a host of other companies offer two-factor authentication or two-step verification. Although these technologies impose an additional inconvenience in exchange for the extra security, they are increasingly mainstream: for instance, Apple now tries to set up two-factor authentication for all Apple Accounts by default, and other companies frequently offer two-factor or two-step verification to users who aren't already using it. These technologies drastically reduce the chances of an account being hacked, because the attacker would need both your password and your mobile device (or other factor). So I heartily recommend enabling that option whenever you can.

I cover both types of expanded authentication extensively in *Take Control of Your Passwords*.

Create Privacy Rules for Yourself

One privacy rule I think everyone should follow is this: *Be suspicious.* Whenever you encounter a request (or demand) to click a link, type (or say) a password, or reveal any other personal information—whether that request came via email or SMS, in a phone call, a messaging app, a

webpage, or even in person—ask yourself whether you're positive that you understand the reason for the request, that you trust the other party, and that revealing that information is truly necessary. The volume and variety of scams I've encountered has made me much more alert to potentially unsafe data collection, and although I don't want you to be paranoid that *every* request for personal info is a problem, it doesn't hurt to take a moment to reflect before giving away your data.

Beyond that, I suggest creating a short list of personal privacy rules.

Some pieces of information (refer back to Things You Might Want to Keep Private) are nearly always private in the sense that you likely want to control who knows them. And there may be some people with whom you almost always want to communicate privately, regardless of the topic—your doctor, lawyer, accountant, therapist, minister, AA sponsor, business colleagues, clients, and so on.

Only you can say what counts as private for you. You can't foresee every situation, but you can identify information and people that deserve extra care when it comes to online privacy. For now, jot down a list of your privacy "triggers." For example, someone might list:

- My credit card numbers
- My new pseudonymous novel
- My chocolate chip cookie recipe
- My mistress
- My attorney
- My FBI handler

Or whatever. Then, as you read this book and learn about the specific privacy risks and options for various types of online communication, you can form these into simple rules, for example:

- I'll never send a credit card number or Social Security number by email unless it's encrypted (*and* I'm confident that the recipient will protect the information on the other end).

- I'll insist that my publisher use encrypted email for discussing "J.K.'s new novel." (No one will guess my true identity!)
- I'll talk about my ____ (invention, legal concern, addiction, etc.) only by phone or in person—never in writing of any kind.
- I'll use an anonymous web browsing tool such as Tor (see Browse Anonymously) when researching competing cookie recipes.

Remove Your Info from Google

Recall from Big Data Is Harder to Get Away From and What I Wish I Could Tell You that Google is near the top of my list of threats to your online privacy. But it's even more difficult for most of us to avoid Google than it is to avoid Facebook. That's because Google isn't just a search engine. It's a vast ecosystem with tendrils running through nearly every device and operating system.

Absolutely avoid Google products if and when you can, but it's unrealistic, in the modern world, to tell anyone never to touch anything that comes from Google, and I wouldn't pretend otherwise. Even if you can't avoid using Google products and services, however, you can tell Google to delete…well, not all of your personal data, but at least an important chunk of it—and to stop collecting data in the future, at least in certain specific situations.

Pause and Delete History

The first thing you can do is pause the collection of certain types of data within your Google account and delete what Google has already stored:

1. Go to the Data & privacy portion of your Google Account page and sign in if you're not already signed in.
2. Scroll down to "Things you've done and places you've been."
3. Under "History settings," click Web & App Activity.
4. Click "Turn off."

5. Click Pause.
6. When the "Setting is off" window appears, click "Delete old activity."
7. Click "All time."
8. Click Delete.
9. Now repeat steps 4–8 with Timeline and YouTube History.
10. Under "Personalized ads," click My Ad Center.
11. Click the On button in the top-right corner of the window, and then click "Turn off." Confirm by clicking "Got it."

If you're thinking, "Wow, that's a lot of hoops to jump through," you're not wrong. Google would *really* prefer that you not do this!

But don't get too comfortable yet; I have to explain what you've actually accomplished. By deleting your existing history and asking Google to stop collecting more data, you've done that *only for your Google account*, which means it affects what happens only *while you're signed in* to your Google account. That's not the same as what's saved in Google's behind-the-scenes profile of you.

Paradoxically, you have to sign in to your Google account—thus enabling Google to specifically track you—in order for Google to honor your requests not to collect any more information about you! So, to the extent that you *must* use Google services that require you to sign in, this is a good thing. But if you follow my advice elsewhere in this book and avoid signing in to Google, nothing changes about their data collection!

For example, Google may not know that John Smith searched for information on air conditioners; they know only that someone whose IP address, browser configuration, and other details happens to match those of a profile already in their system searched for that information. And it could *just so happen* that, somewhere along the line, the person matching that profile also entered the name John Smith or the email address iamjohsmith@gmail.com on a Google-owned website, the

result of which is…yeah, Google knows exactly who it was, and they would be more than happy to show that person air conditioner ads.

I'm saying that deleting your data from Google and turning off their data collection gives you the false impression that they're not tracking you. They are, they're just not associating that tracking data with your Google account. Better than nothing, sure. But probably not what you were hoping for.

Results About You

Another thing Google lets you do—which is probably worthwhile although, again, not as complete as you may prefer—is to remove personal information about yourself from Google search results. For example, if someone searches for your name and one of the pages that pops up contains your phone number or physical address, you can ask Google to stop including those pages in search results for your name.

To do this, go to Google's Results about you page. Sign in if you haven't already done so, click "Get started," and follow the prompts. I'm sorry to say that the process is rather tedious and involved, and that ultimately all you can do is submit a removal *request*. You can't force Google to remove any results, and this process doesn't prevent other private information about you from showing up in future searches.

Also, I want to be clear that you're not removing the pages with your personal information from the web, or even from Google's search index. Those pages will still be there, still findable in other ways or through other search engines. This process merely makes them stop appearing in Google searches.

So, once again: better than nothing! Worth doing! But still not great.

Purge Your Info from Data Brokers

Earlier, in the discussion of Data Brokers, I explained how huge companies profit by collecting and selling all sorts of personal data about you—much of it collected as you surf the web, post on social media,

and use the internet in other ordinary, day-to-day ways. I also said that Doxxers can tap into this data in order to make private details about you public—but, of course, advertisers, government agencies, and anyone else with money can also access this information.

I wish I could tell you that you can easily remove your information from all these databases, but data brokers intentionally make the opt-out process obscure and difficult—if they even offer it at all. (In most cases, laws give such corporations wide latitude to do whatever they want with your data.) If you can opt out of a given data broker, it may require anything from filling out a form online to mailing or faxing a letter along with a copy of your photo ID. And there are *hundreds* of data brokers that may have your personal information.

Fortunately, journalists and other researchers have compiled lists of data brokers, including how to opt out (if at all). There's some overlap in these lists, but each one adds interesting details, so I suggest checking them all out:

- Big Ass Data Broker Opt-Out List by Yael Grauer at GitHub
- Here are the data brokers quietly buying and selling your personal information, by Steven Melendez And Alex Pasternack at Fast Company (the most comprehensive list I've found so far)
- How to opt out of Facebook data sharing by Joseph Keller, at iMore
- How to Opt Out of the Sites That Sell Your Personal Data by David Nielo, at Wired

Note: One service that's mentioned on none of these lists but is notorious for giving unwanted people access to your private data is FamilyTreeNow. You can (allegedly) remove yourself on the site's Opt Out of Records page, but I've heard reports that users' data wasn't deleted following a request.

Opting out from even a fraction of these brokers will involve considerable time and frustration—and for all that, it's no guarantee, because many brokers don't let you opt out at all, while some brokers honor requests to delete the data they already have about you yet don't stop

collecting more in the future. And bear in mind brokers' opt-out procedures involve turning over your personal information to organizations you've already decided you don't trust. But if you're serious about protecting your online privacy, it can be in your best interest to reduce the number of entities tracking and storing your information.

Unsurprisingly, lots of sites, services, and apps have sprung up to address this problem: they'll track down as many data brokers as they can who have your personal data, submit all those complicated opt-out requests on your behalf, and monitor the brokers in case your data reappears there in the future. For a fee. Often, a rather large fee. Because one way or another, you have to feed the machine.

Do I sound a bit cynical and bitter? I am a bit cynical and bitter. But the fact is, either you do a lot of tedious work yourself, or you pay someone else to do it for you. If you have more money than time, here are some examples of the many data-removal tools you can consider:

- DeleteMe purports to remove your data from hundreds of data brokers—and repeats the process as needed. Prices start at $129 per year for one person. Available in the United States, Canada, the United Kingdom, Australia, and a handful of other countries.

Note: Although DeleteMe is popular and its marketing materials sound enticing, it ranked near the bottom in a Consumer Reports study (PDF) of search removal services.

- EasyOptOuts claims to remove your data from "over 160 websites" for $19.99 per year. It appears to require a U.S. address.
- Incogni, by the makers of the Surfshark VPN, currently monitors 164 data brokers and submits opt-out requests on your behalf. The price is $12.98 per month or $77.88 per year. It's available to residents of the United States, Canada, the United Kingdom, the European Union, and several other countries.
- Mozilla Monitor Plus searches for your personal data across 190 data broker sites, as well as checking for info that may have leaked

due to data breaches. It costs $13.99 per month or $107.88 per year. Available to U.S. residents only.

Note: Monitor Plus previously included a data removal service called Onerep, but Mozilla ended that partnership when they learned that Onerep's CEO had ties to…a data broker. You can't make this stuff up.

- Optery has plans ranging from $3.99 per month (for removal from "85+ sites") to $24.99 per month (for removal from "605+ sites). Only U.S. residents can use the service at present.
- Permission Slip by Consumer Reports is a free (donations requested) smartphone app that monitors an unspecified number of sites for your personal information and sends opt-out requests. The first thing the app asks you after you sign up is which U.S. state you live in; you can't proceed without answering.

Cope with Special Cases

Online privacy gets tricky when you encounter a situation you weren't expecting—one that isn't covered by your up-front fixes, ongoing habits, and regular rules. For example:

- You win the lottery, and suddenly you have a thousand new "friends" who want a piece of the action.
- You find yourself embroiled in a messy divorce.
- You witness or are otherwise close to a newsworthy event that results in reporters, lawyers, and scammers crawling out of the woodwork and paying you special attention.
- You find yourself in a delicate position involving your health, your insurance, and your employer.
- You or a family member are suspected of a crime.
- You have a fleeting error in moral judgment that may turn out to have far-reaching consequences.

In these and many other situations, your online actions could become subject to much greater scrutiny than normal—you now have to worry about being targeted personally.

No one likes to think about these things, but they do happen, and you're more likely to get through them unscathed if you've spent at least a little time thinking about the online privacy implications in advance.

My first piece of advice is: If humanly possible, avoid saying *anything* about the situation online in any way. The less digital information you generate that could come back to haunt you, the better.

Second, however tempting it may be, don't go crazy deleting things, shutting down accounts, ditching equipment, and the like. That looks suspicious, and could draw unwanted attention to your actions. (Besides, it won't matter, because nothing ever truly disappears from the internet.)

Third, if the situation has any legal implications whatsoever, find yourself a good lawyer and follow their instructions to the letter.

After doing all those things and allowing yourself some time and mental space to think about your situation clearly, if circumstances permit (and your lawyer, if any, agrees), consider cranking all your privacy settings up to 11. That is, go back to everything in this book that you decided wasn't worth the effort or was too inconvenient, and do it anyway, paying particular attention Additional Resources for High-Risk People (and the related sidebars throughout this book). Use a reliable VPN all the time. Use only Tor (see Browse Anonymously) for web browsing. If you're an Apple user, turn on Advanced Data Protection and Lockdown Mode (both covered in the next chapter). Limit your email to completely commonplace, uncontroversial topics. Avoid Facebook and other social media, at least until the situation stabilizes.

I hope you never find yourself having to take such drastic measures. (Unless you win the lottery, because I can totally help you out there.) But if you remember that online privacy is inversely proportional to your need for it, you'll be in much better shape.

That sets the stage for the next topic: avoiding stupidity online.

Take the Pledge

Regardless of what measures you take to protect your privacy, there are certain things that should never, ever, under any circumstances, be sent over any network. I would have thought this is obvious, but judging by frequent news reports, politicians, actors, professional athletes, and other celebrities still haven't gotten the memo that online privacy is the exception rather than the rule.

You don't have to be rich or famous to have your life ruined by online stupidity. Anyone with fingers and a web browser can find millions of photographs, videos, comments, email messages, Facebook posts, and other digital artifacts showing humans at their worst. And more often than not, this stuff is put online *deliberately* by the very people who stand to lose the most…

"Look how fast I can drive this train!" boasted a railway engineer online before recklessly causing a derailment that killed dozens of people.

"I'm sure my wife won't mind a bit of harmless online flirting with other women," said a public official whose wife—and constituents—turned out to mind very much.

"Stealing this car will be a piece of cake," said the guys whose every movement was being recorded on dozens of traffic cams.

"Why, yes, I think it would be a great idea for me to post a video of our drunken college orgy!" said a young lady who will find it difficult to get any respectable job in the future because her prospective employers know how to use a search engine.

Folks, the very best decision—for you and for the rest of the world—is to *stop doing stupid things*. But if you are going to do stupid things anyway, don't compound your stupidity by putting evidence of it on the internet, which, as you'll recall, never forgets. As you've seen already and will learn in more detail throughout this book, it's nearly impossi-

ble to guarantee complete online privacy—and the worse you behave, the more likely it is that evidence of your behavior will emerge.

So, I'm not merely going to tell you to refrain from putting potentially incriminating information about yourself online. I'm going to ask you to *promise* me not to be stupid online. I ask you to join me in taking The Pledge.

Turn on your webcam, raise your right hand, and repeat these words:

> *I, (state your name), do hereby solemnly affirm before the all-seeing, all-remembering eye of the internet that I will never, ever, under any circumstances, for any reason, or in any manner, knowingly cause or permit any of the following information to travel over any network:*
>
> 1. *Statements that are hateful, abusive, racist, or otherwise cruel*
> 2. *Nude or sexually suggestive pictures or videos of myself, my friends, my family, current or former romantic partners, or anyone else who might at some point deserve to have a life*
> 3. *Information that could implicate me, rightly or wrongly, in any crime*
> 4. *Any material that violates someone else's copyright, patent, or other intellectual property*
> 5. *Anything I'd be ashamed for my (current or future) children to see or hear*
>
> *I further acknowledge that any failure to keep this pledge could disqualify me from ever holding political office, practicing law or medicine, teaching in a public school or university, holding any government or public sector job, owning a puppy, living in a nice home, finding (or keeping) true love, receiving technical support, enjoying ice cream, or pretty much anything else that might bring me happiness.*
>
> *I therefore, voluntarily and without coercion, undertake to avoid extreme online stupidity for the rest of my days.*

Remember my motto: *What happens on the internet, stays on the internet*. Don't assume you can erase or fix something later. The only way to be sure your stupid thing won't live on forever in internet infamy is not to put it online in the first place.

When Privacy Hurts

For the most part, I assume more privacy is better than less. But there are counterexamples—situations in which you'll be safer or happier with *less* privacy. For instance:

- You know how you use Caller ID on your phone to tell you who's calling so you can answer when it's a friend and send the call to voicemail if it's someone you don't want to talk to? Well, the people *you* call use it the same way. So if you disable Caller ID for outgoing calls, you may get a teensy smidgen of extra privacy, but you also greatly increase the risk that people won't pick up because they won't know it's you.
- If you try to get a reservation with Airbnb, the host may want evidence that you're someone reasonable enough to invite into their home. Profiles with your real name and information about your real college, job, friends, and background could put someone at ease, while a fake profile (or none at all) could put them off.
- The same employers, insurers, lenders, and other institutions that could ding you for negative information in social media could reward you for positive information.
- New friends might feel more comfortable letting you into their lives if they can find out more about the real you online. Similarly, you might find it difficult to keep up with old friends who, for whatever reasons, embrace services and social media and services (like Facebook) that you're not comfortable with.
- If the police want to know where you were on the night of the 16th, you might be able to point them to exculpatory photos or posts—but you better be able to prove they're really yours!

I can't make any blanket statements about what you should or shouldn't keep private; I can only say, as I said before: privacy cuts both ways.

Keep Yourself Informed

As I've mentioned, online privacy is best thought of as a process. You'll make changes, the bad guys will come up with new attacks, technology companies will develop new defenses (which will require you to update your software and rejigger your settings), and the cycle will continue forever. No matter what you do today, your privacy may still be at risk tomorrow. So, I recommend strongly that you stay alert, pay attention, and seek out information that can help you avoid or address new threats before they become serious.

Here are some ways you can stay informed:

- **Keep your software up to date.** This includes your operating systems themselves and any third-party apps, but especially those with security or privacy implications. When a new update becomes available, you should read (or at least skim) the release notes to become aware of what bugs were fixed or privacy concerns addressed. (You should also, of course, be on the lookout for any changes that might *decrease* your privacy!)
- **Watch your bank accounts.** Check your bank, credit card, and investment accounts regularly, keeping an eye out for unexpected charges or unknown vendors. Since one of the big reasons attackers try to discover private information about you is to steal your money, it's in your best interest to notice any financial malfeasance early so that you can inform your financial institutions and (if applicable) law enforcement to take action.
- **Read the news.** Maybe reading technology-oriented news sites isn't your idea of a good time, but even conventional news sites routinely report on major scandals, lawsuits, data breaches, and other events that could affect your privacy. Pay attention to them.

  A great recent example is a series of news stories about Microsoft's Recall, part of Windows 11 that works only (for now) on the company's Copilot+ PC line. Recall keeps track of everything that happens on your device—what you type, the files you open, the photos you

view, the websites you visit, and so on—with the ostensible goal of making it easier for you to find your own stuff later. OK, but that stored data could also be a tempting target for hackers, and you'd be right to think twice about using it.

- **Monitor your passwords.** Sites like Have I Been Pwned? and password managers like 1Password (refer back to See How Bad Things Are) can tell you whether your email addresses or passwords have been found in data breaches. You should immediately change passwords on any services impacted by the breach.
- **Check for updates to this book.** I've updated this book numerous times, and plan to continue doing so in the future (though not, perhaps, as frequently as I would like). I'll do my best to include the newest and best advice each time. (See Ebook Extras.)

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

earlier); in iOS/iPadOS, go to Settings > *your name* > iCloud > Hide My Email.

Note: iCloud+ subscriptions start at just 99¢ per month.

In Mail, you can now simply click or tap the "From:" field when composing a message and choose Hide My Email (**Figure 1**). Mail does the rest of the job and fills it in for the email message (**Figure 2**). The entry appears immediately in the Hide My Email list in all your iCloud-associated locations.

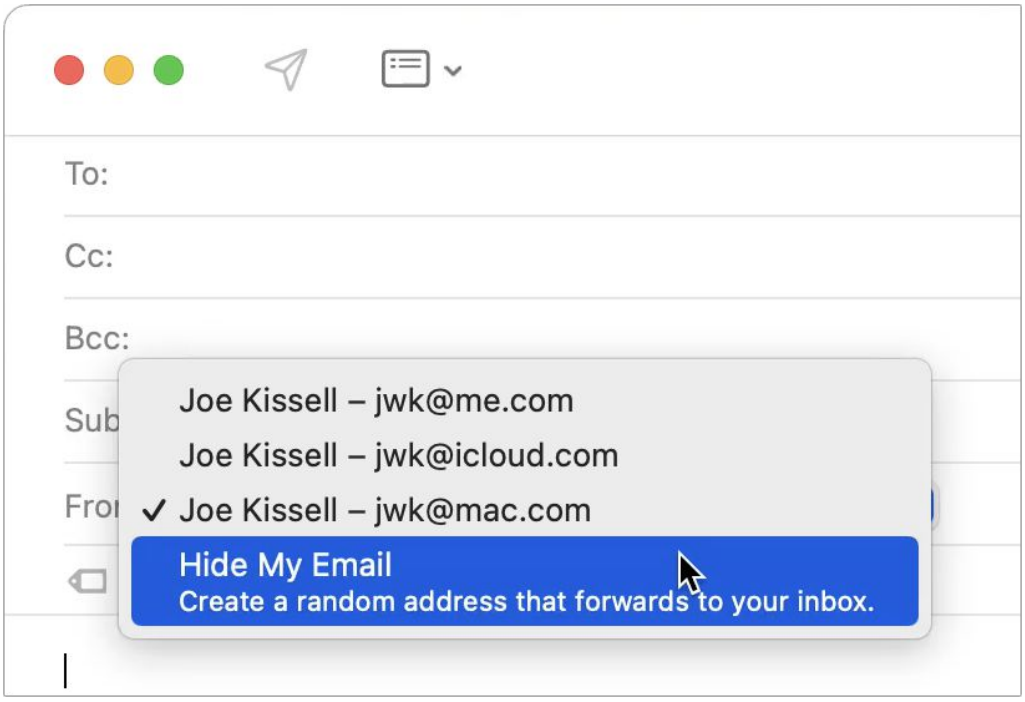


Figure 1: Select Hide My Email from the "From:" menu in an outgoing message and macOS generates an address automatically.

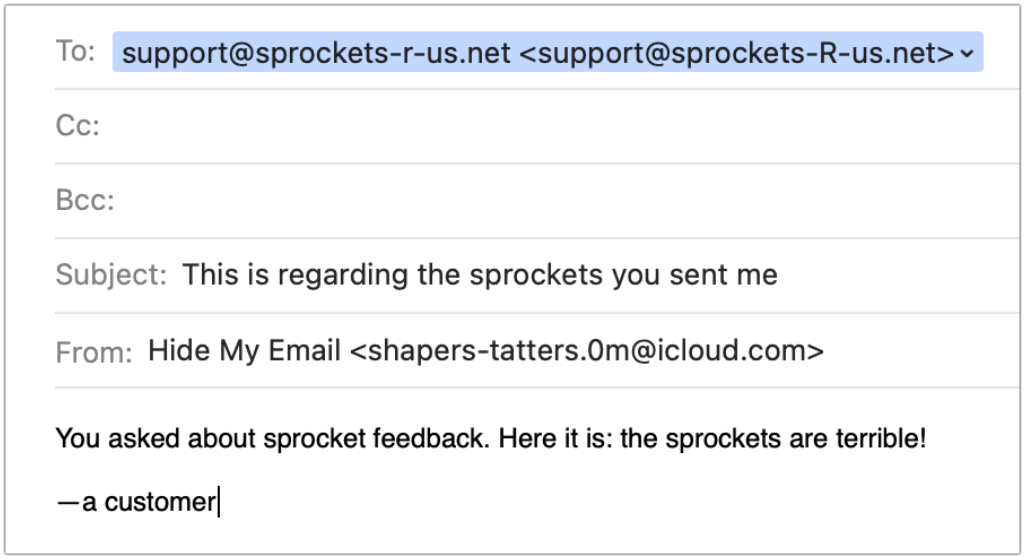


Figure 2: The composed message has the email alias filled in and identified to you (not the recipient) as using Hide My Email.

Mail Privacy Protection

The Mail Privacy Protection feature in Apple's Mail app for macOS, iOS, and iPadOS makes it harder for people and companies to track you through email. (At least it does in theory; read on for a significant qualification.)

When you enable this feature, by default, Mail downloads any remote images in email messages in the background, using an Apple server elsewhere on the internet rather than your personal device. This means that, if the message includes a tracking pixel (see Tracking Beacons), loading the image signals to the sender *that* you opened it, but not precisely *when* you opened it, *how many times* you opened it, *where* you opened it, or whether you forwarded it. (And, because the sender doesn't know your real IP address, they can't use that, in combination with web tracking, to build up their profile of your behavior.)

To enable Mail Privacy Protection, do the following:

- **macOS:** Go to Mail > Settings > Privacy and select Protect Mail Activity.
- **iOS/iPadOS:** Go to Settings > Apps > Mail > Privacy Protection and turn on Protect Mail Activity.

However, weirdly, Mail Privacy Protection still *does* load those tracking images, and therefore still *does* tell the sender that you, specifically, received the message. If the sort of privacy you're looking for includes hiding from senders the fact that you received and opened their messages at all, you won't get that without some extra effort. To do so, counterintuitively, you have to *disable* Protect Mail Activity in the above locations. Once you do so, two more options appear:

- **Hide IP Address:** This feature sends any requests for remote content (typically embedded images, which may include the invisible tracking pixels) through proxy servers to prevent the sender from knowing your IP address and location. In other words, this is a portion of Mail Privacy Protection, but not including the automatic background loading feature. I suggest enabling this feature.
- **Block All Remote Content:** This setting prevents Mail from downloading embedded images and other content automatically at all, though you can still load such images manually, if you like. I also suggest enabling this feature.

When Block All Remote Content is enabled, Mail hides all remote graphics in an incoming message (that is, graphics that aren't embedded in the message itself) and displays a banner at the top of such messages along with a button or link allowing you to manually load those images. (In macOS, the banner says "This message contains remote content," accompanied by a Load Content Directly button; in iOS/iPadOS, the banner says "Message contains unloaded images" and is followed by a Load All Images link; see **Figure 3**.) But remember: if you do load those images, you tell the sender that you've done so—and exactly when.

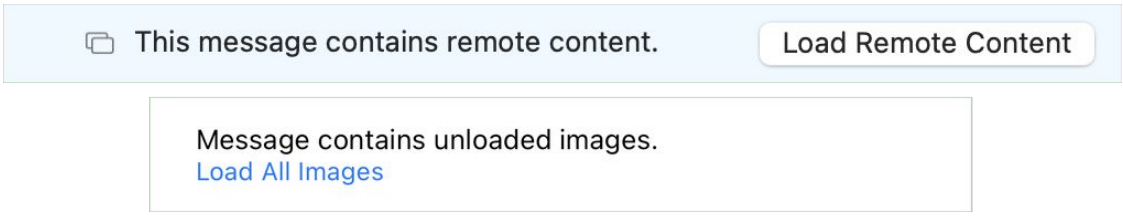


Figure 3: This message has Block All Remote Content enabled. macOS shown at top; iOS at bottom.

Link Tracking Protection

macOS 14 Sonoma and later, and iOS 17/iPadOS 17 and later, have a feature called Link Tracking Protection**.** If you use either the Mail or Messages app to share a URL from a website, the operating system strips out extra information that's used to track you across the web (without hindering the URL's functionality). This is automatic; there's nothing to set, nor can you turn off this feature.

Intelligent Tracking Protection

Intelligent Tracking Prevention in Safari automatically prevents tracking cookies from being shared with third-party sites after 24 hours, and deletes them entirely after 30 days. (That's still too generous for my taste, but it's a step in the right direction.) To enable this feature on a Mac, choose Safari> Settings > Privacy and select "Prevent cross-site tracking." On an iPhone or iPad, go to Settings > Apps > Safari and turn on Prevent Cross-Site Tracking.

Privacy Nutrition Labels

Since mid-2022, the App Store for iOS, iPadOS, and macOS has included Privacy Nutrition Labels at the bottom of each app's listing (**Figure 4**) that tell you what sort of data the app may collect and whether that data is linked to you, personally. Each app may have any or all of the following sections: Data Linked to You, Data Not Linked to You, and Data Used to Track You; under each heading, as many as 14 different kinds of data may be listed.

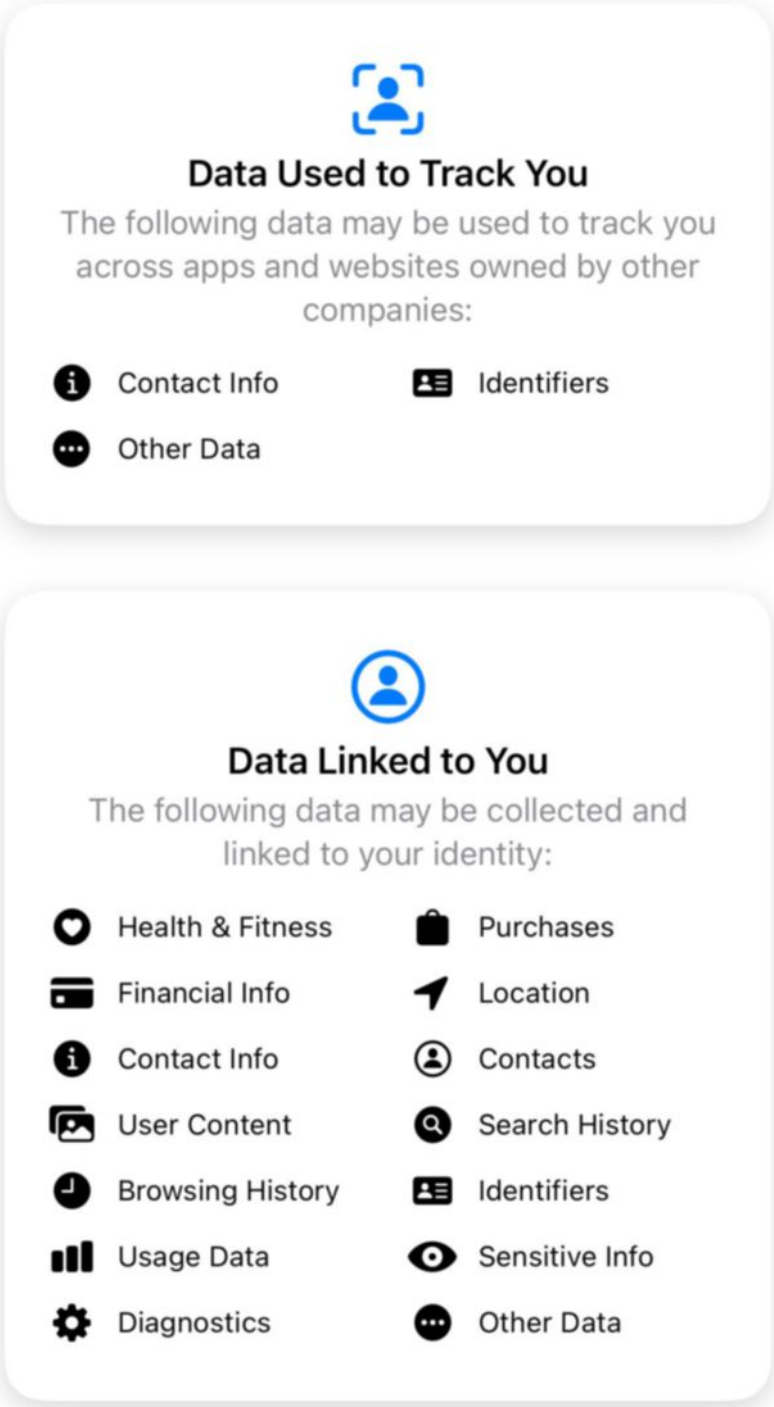


Figure 4: Privacy Nutrition Labels tell you what sort of personal information an app will try to collect.

Tap one of those sections to see more precise details. For example, if an app collects contact info, the detailed view might tell you that includes physical address, email address, name, phone number, and other user contact info.

The image shown above is from the Facebook app for iOS. Even without the detail view, you can see that the app wants to collect every imaginable piece of data it can. I'm sure you're just shocked about that.

Even though these labels describe what the app *wants* to collect, you can still turn off *some* (but not all) types of data collection. On an iPhone or iPad, go to Settings > Apps > *App Name* and Settings > Privacy & Security > Location Services. On a Mac, go to System Settings > Privacy & Security and browse the various categories.

App Privacy Report

Taking the information from privacy nutrition labels a step further, iPhones and iPads also have an optional App Privacy Report you can (and should) enable that monitors apps' usage of your device's data, sensors, and network activity so that you can keep track of exactly what apps *have* done, which might be different from what they *should* do.

To use it, go to Settings > Privacy & Security > App Privacy Report and click Turn On App Privacy Report. Then go about your business as usual for a while and check back in the same location to see what data apps have collected recently.

Location Tracking Protection

One important privacy category, especially for iPhones, is your location, which many apps want to know. (I say more about this later, in Location Awareness.) Although some apps have an excellent reason to know your location (such as navigation, workout, and weather apps), apps often ask for more information than they actually need—or, at least, more than you're willing to disclose. You have several options for fine-tuning what location data is shared with various apps. Go to Settings/System Settings > Privacy & Security > Location Services to configure them:

- To prevent any app (or the operating system itself) from disclosing your location for any reason, turn off Location Services at the top.

(Normally, however, you'll want to leave that on and restrict access more granularly.)

- On an iPhone or iPad, tap Share My Location to configure how your device's location is shared with the Find My app, family, and friends. (On a Mac, you can enable/disable Find My Mac in System Settings > *your name* > iCloud > See All (or Show More Apps) > Find My Mac; family location sharing settings are in System Settings > Family > Location Sharing.)
- On a Mac, you can turn location services on or off for each app. On an iPhone or iPad, tap an app name to specify location settings for that particular app:
  - In the Allow Location Access section, select the conditions under which the app may access your location. Depending on the app, choices may include Never, Ask Next Time Or When I Share, While using the App (usually the most convenient option), or Always.
  - Turn Precise Location on (the default) to let the app know *exactly* where you are; turn it off to provide only your general location—an area of about 10 square miles or 16 square kilometers.
- At the bottom, tap System Services (iOS/iPadOS) or click Details (macOS) to display more than a dozen switches that let you provide your location to, or hide it from, specific features within the operating system.

iCloud Private Relay

Like Hide My Email, iCloud Private Relay requires a paid iCloud+ subscription. This feature is *almost kinda sorta* like a VPN, in that it encrypts internet traffic traveling to and from your Mac and prevents websites you visit from tracking you by hiding your IP address (and, in turn, your true geographical location). iCloud Private Relay uses two separate relays operated by Apple when you visit a site in Safari, ensuring that no one can know both *who* you are and *where* you are.

Remember: unlike a fully-featured VPN, iCloud Private Relay works only with Safari and a limited number of other internet services (such as DNS lookups). So it won't protect *all* the internet traffic on your Mac, iPhone, or iPad, but as far as it goes, it's an excellent idea.

To enable iCloud Private Relay, go to Settings/System Settings > *your name* > iCloud > Private Relay and turn the switch on. Once it's enabled, you can use the IP Address Location pop-up menu to choose either "Maintain general location" (to give websites an approximate idea of where you are—useful if you're ordering takeout or checking the local weather) or "Use country and time zone" (if you'd rather keep your location a bit vague).

Note: You can't have both iCloud Private Relay and a VPN active at the same time.

Advanced Data Protection

Apple's iCloud data security review page provides a nice summary of which types of data your iCloud account encrypts. To make a long story short, some things are encrypted only in transit and on the server while others are encrypted end to end (see the sidebar ahead). Some items that support end-to-end encryption are handled in such a way that Apple *could* decrypt them if they were legally required to do so, because the encryption key is stored on Apple's servers rather than on your own trusted devices.

You have the option to encrypt *more* data types end to end—and you should use it if you can. (Presumably, the option isn't turned on by default for everyone because it has a bunch of prerequisites that not everyone can meet, as I explain in a moment.)

This feature is called Advanced Data Protection (ADP). When you enable ADP, Apple uses end-to-end encryption for nearly all the data that would otherwise have been encrypted only in transit and on the servers. This includes iCloud backups (see Mobile Backups), Find My, iCloud Drive, Messages in iCloud, Notes, Photos, Reminders, Siri

Shortcuts, Voice Memos, and Wallet passes. (Email, contacts, and calendars remain unencrypted, even with this feature enabled, because of the inherent design of the systems used to transfer that data.)

What's End-to-End Encryption (E2EE)?

Encryption is great for your privacy, but that encryption may not extend all the way from one end (you, or one of your devices) to the other end (another person or device). For example, if your email app uses an encrypted connection to your mail server (it probably does: see the sidebar Log In and Transfer Email Securely), messages you send are encrypted *while in transit* between your device and the mail server. But they're not necessarily encrypted on the mail server or on the rest of their journey to the recipient.

By contrast, if a message, file, or other data is encrypted on your device, and it's decrypted only on the recipient's device, that's end-to-end encryption (E2EE). Of course, once the data has been decrypted, the recipient might not keep it private, but that's true of all encrypted data.

Before you can enable ADP, all of the following must be true:

- *Every* device signed in to your iCloud account must be running at least macOS 13.1 Ventura, iOS 16.2, iPadOS 16.2, tvOS 16.2, watchOS 9.2, or HomePod 16.2.
- You must have two-factor authentication enabled for your Apple Account.
- Passcodes or passwords must be set for all your Macs and iOS, iPadOS, and watchOS devices.
- You must have a recovery key or a recovery contact—or both.

Once you've met all those criteria, you can enable ADP. To do so, go to System Settings (macOS) or Settings (iOS/iPadOS) > *Account Name* > iCloud > Advanced Data Protection. Click Turn On (macOS) or tap Turn On Advanced Data Protection (iOS/iPadOS). If you have any devices signed in to your iCloud account that don't meet Apple's criteria, a message tells you, for each of those devices, whether you can update it or must remove it from your account.

Assuming that's all good, Apple verifies your account recovery setup:

1. A message reminds you that Apple will no longer be able to recover any of the data you're about to protect—that's your responsibility now. (And if you haven't already set up one or more recovery methods, you're prompted to do so now; you can't proceed otherwise.) Click or tap Review Recovery Methods.
2. If you have a recovery key, enter it, click or tap Next, and enter your device's password or passcode when prompted.
3. When "Advanced data Protection is On" appears, click Done.

Apple also sends email to your iCloud.com address confirming that ADP is now enabled.

Lockdown Mode

As the list above indicates, Apple devices offer a great many privacy features, though not all are enabled by default. However, even with every one of those features turned on, a determined attacker could conceivably exploit unknown weaknesses in Apple's hardware or software to obtain your private information (or even threaten physical violence). And so, for the most serious situations, such as journalists, activists, and government officials who are very likely to be targeted, Apple offers an even stronger option: Lockdown Mode.

With Lockdown Mode enabled, Apple strictly limits a fairly long list of features on your device. For example, most attachments in Messages are blocked, potentially suspect web technologies are disabled, location information is stripped from photos you share, and explicit permission is required for a number of activities. All these restrictions make it much harder for someone to remotely track you, install spyware, or steal your personal data; they also will very likely make it more inconvenient for you to use your own device, though it is possible to exclude particular apps and websites (in Safari) from Lockdown restrictions.

Apple provides complete details about what Lockdown Mode does and how to activate or deactivate it in About Lockdown Mode.

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.)

And those sorts of concerns merely involve the historical record. Day-to-day social media posts can also cause privacy problems:

- You mention on X that you're going on vacation (or just going to a concert), and burglars break into your house. Or, even worse, you post an image of an expensive object you just acquired, which then makes your home that much more of a target.
- You post geotagged pictures on Flickr that show your location and the time you took them—today, just after you called in sick to work.
- Your Facebook relationship status says "It's complicated," but your romantic interest didn't think so.

You get the idea, I'm sure. The stakes when it comes to social media are much higher than you may imagine. Your social media history can win you—or cost you—a job, love, or even your freedom.

Learn About the Facebook Problem

But it's not just the things you *post* that could cause you grief. There's an even bigger underlying issue.

Folks, we need to have a little talk about Facebook. Yes, there are other huge companies (including other social media companies) that collect an obscene amount of personal data. But Facebook—whose parent company, Meta, also owns Instagram, Threads, and WhatsApp—stands out as an extreme example, not only in the volume of information it absorbs but also in its repeated and blatant disregard for privacy, transparency, and accountability.

In fact, I don't think it's an exaggeration at all to say that the number one thing you could do to improve your online privacy is to *stop using Facebook*. I realize that, to many people, that may sound like "the number one way to lose weight is to stop eating," which is to say, perhaps true in principle but unworkable in practice. I completely understand. But if you choose to continue using Facebook, I want you to understand the risks (and reduce them as much as possible). We'll get to all that in a moment.

In case you're unaware of the extent and nature of Facebook's issues, let me give you just a *tiny* sampling:

- In 2018 it was revealed that Facebook's Onavo VPN service enabled the company to spy on nearly all the internet data of its users, many of whom were teens—some of them actually paid in gift cards in exchange for letting Facebook watch all their online data. Under public pressure, Facebook eventually shut down Onavo. Even then, the company initially said that less than 5% of Onavo users had been teens, but was later forced to admit that the number was 18%. Later still, documents that were released as part of a lawsuit showed that Facebook used Onavo to read encrypted data from Snapchat (which Facebook viewed as competition) as well as YouTube and Amazon.
- Shortly thereafter, Facebook was at the center of the Cambridge Analytica data scandal, in which an outside data broker was permitted to gather private data from tens of millions of Facebook users without their knowledge or permission and use it for political purposes.
- Facebook was also shown to be a major platform for Russian and Iranian trolls attempting to use propaganda influence the 2016 U.S. election. Facebook was also used to spread propaganda that contributed to the possible genocide in Myanmar.
- Researchers discovered that when you set up Facebook's two-factor authentication (see the sidebar About Two-Factor Authentication, earlier) to send login codes to a mobile phone number, that phone number can also be targeted by advertisers; in early 2019, it was revealed that phone numbers used for two-factor authentication are also fully searchable, presenting a significant privacy risk and even physical danger to some Facebook users. Facebook is also using other aspects of your contact information in ways that are not disclosed to users—and that you can't opt out of.
- Facebook has asked some users for their email passwords in order to create an account—something Facebook should never need.

Facebook says they ended the practice in early 2019, but only after it was publicly disclosed by a security researcher.

- A security breach reported in October 2018 revealed information such as phone numbers and email addresses for nearly 30 million Facebook users, as well as more personal information (such as relationship status, religion, and a partial search history) for nearly half of them.
- Then, in late 2018, a Facebook software bug reportedly exposed as many as 6.8 million users' private photos to app developers.
- In February 2019, a variety of third-party mobile apps were found to be covertly sending personal data to Facebook. And when I say "personal," I mean things like users' heart rate info, menstruation data, and the addresses of real estate listings the users were considering.
- Arielle Paredes, writing for Wired in 2020, described how Facebook uses sneaky user interface tricks (widely termed "dark patterns") to manipulate users into agreeing to give away more of their private data than they intend.
- A 2021 report showed that Facebook (and Instagram) stripped location data from photos users uploaded, while keeping and using that data as part of the user's advertising profile.
- In early 2024, an extensive study showed how nearly 200,000 different companies send personal information about their own users to Facebook, even when those people weren't using the Facebook website or all—and without their knowledge or consent.
- Facebook and Threads blocked an entire news site in April 2024 after it posted a story showing how Facebook refused to let users boost stories about climate change.

Facts like these (and many, *many* more) have led respected journalists and pundits to say some pretty strong things. Walt Mossberg says Facebook CEO Mark Zuckerberg has never cared about privacy. John Gruber goes further, repeatedly referring to Facebook as a criminal

enterprise. Rene Ritchie at iMore thinks you should Delete your Facebook. And even Roger McNamee, an early Facebook investor and mentor of Zuckerberg, wrote a book called *Zucked* that's devoted to "stopping Facebook from destroying our democracy."

In a March 2019 post, Zuckerberg claimed he was going to take Facebook in a new, privacy-centered direction. But that was self-evidently false, because Facebook's entire business model is built on the very opposite of privacy. Indeed, if you read that post carefully, you'll see that Zuckerberg never says Facebook is going to stop collecting personal data and using it to show you ads, only that Facebook would develop more and better ways of exchanging encrypted messages. Big. Deal.

Facebook has shown itself over and over again to be untrustworthy, even regarding the *most basic* aspects of data security—in early 2019 researcher Brain Krebs revealed Facebook had been storing hundreds of millions of Facebook and Instagram user passwords in plain text, available to thousands of employees, for the better part of a decade. It's clear that revenue is not only more important to Facebook than privacy, it's the *only* important thing.

As the examples above show, it's not enough to lock down Facebook's privacy settings (though you should certainly do that anyway; every little bit helps). Reducing your number of Facebook friends or the frequency of your posts won't solve the problem either. As long as you have Facebook, Instagram, or Threads accounts, you should assume that the company is slurping up every last bit of personal data about you that it can—*and* sharing it with anyone and everyone.

Facebook is very bad news for your online privacy, no two ways about it. Some people, upon learning this, delete their Facebook accounts and never look back. Good for them! If you feel that's a reasonable option for you, and that you can find other ways to keep in touch with people and do the sorts of things you depend on Facebook for, I encourage you to do just that.

But…

I also know that Facebook is indispensable for some people. For example, there are community organizations, support groups of all

kinds, messaging groups for extended families, and entire businesses that depend exclusively on Facebook for their existence. It's all well and good for me to say you should stop using Facebook, but if a group that's important to you relies on Facebook and is unable to meet its members' needs in any other way, you may have to face an impossible choice: keep feeding Facebook's database or cut off essential relationships and communication.

I get it. And I can't tell you what you should do, but it's my obligation to lay out the facts so that you can make a decision with both eyes open.

Realistically, I imagine most of you are going to keep using Facebook, and that will be my assumption for the remainder of this chapter. I do urge you to take as many steps as possible to mitigate the problem, which includes not only adjusting your Facebook settings, as I describe next, but also locking down your internet connection and web browser (as I discuss in the next two chapters), which can put a dent in the amount of information Facebook is able to collect.

Check Your Privacy Settings

Every social media site and service has a privacy policy (see What About Privacy Policies?). You should read it, if only to be aware of how much data you're inevitably giving away.

Beyond that, examine each account's privacy settings. Some services offer very little privacy control—and the controls they do offer are based on keeping your content private from particular people, but not, obviously, from the service itself (or its advertisers). Facebook has changed its privacy settings repeatedly. The Meta Privacy Center, which covers Facebook, Instagram, and Messenger, currently offers at least the appearance of control (**Figure 5**), letting you limit who can see various categories of information (for example, everyone, only friends, or friends of friends)—but even limiting sharing to your friends is no guarantee that one of those friends won't share it, or that

a programming error or misbehaving app might not reveal it (which has happened repeatedly, as discussed above).

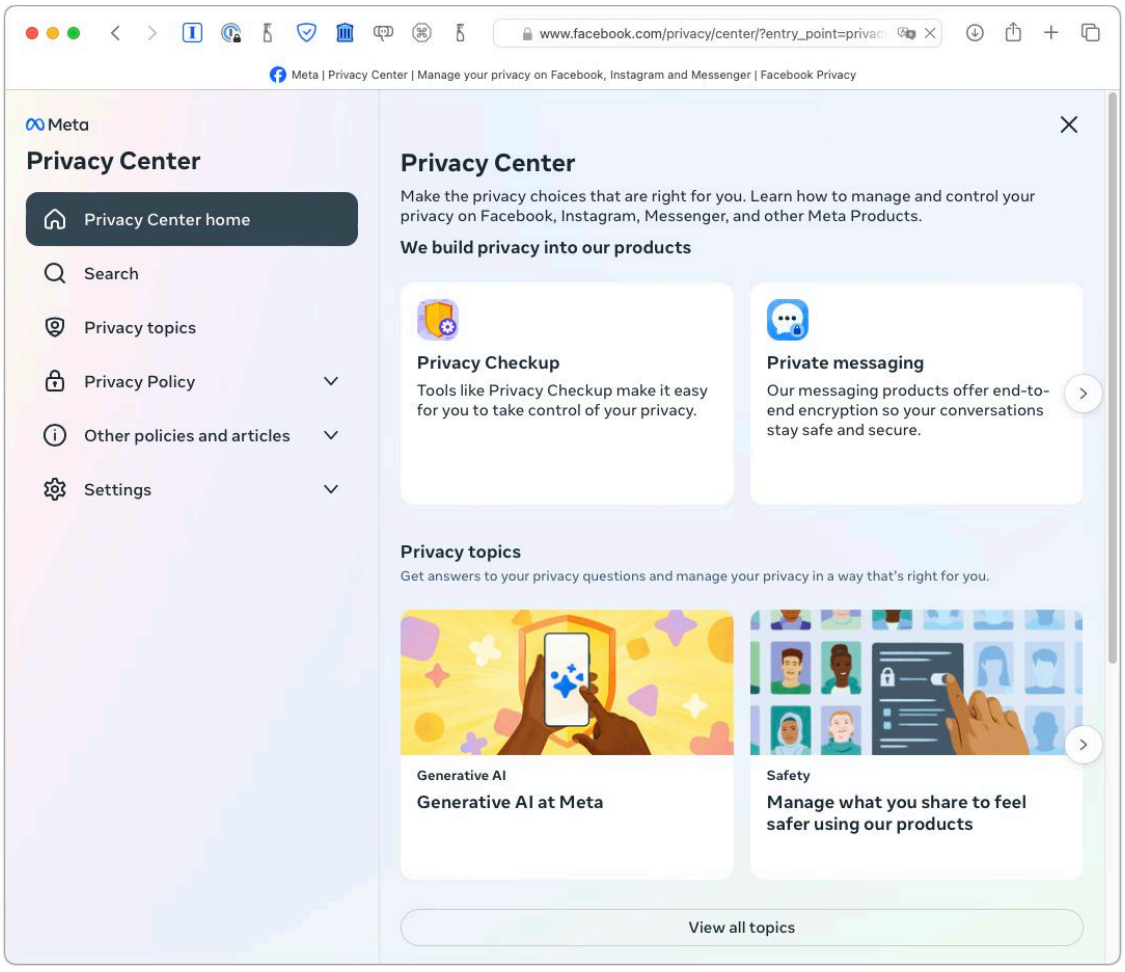


Figure 5: Meta's privacy settings are less detailed than many would prefer—and, let's face it, probably can't be trusted—but they're better than nothing.

In other words, do pay attention to the settings and configure them as best you can, but don't count on them. They are neither foolproof nor trustworthy.

Here are direct links to access the privacy settings for a few popular social networks:

- Bluesky
- LinkedIn

Note: Mastodon is not a centralized service, so all settings must be managed on whichever Mastodon instance you use.

- Meta (Facebook, Instagram, Messenger)
- MySpace
- Pinterest

Note: Threads, which is part of Instagram (and thus part of Meta) doesn't offer a way to manage privacy settings on a webpage; instead, you must change the settings in the Threads app.

- X (formerly Twitter)

Note: Although Google is not a social media service, it will certainly ingest anything you post on social media. Refer back to Remove Your Info from Google.

Use Other Social Media Precautions

Apart from the obvious advice not to post anything on social networks that you'd mind being public (even via "private" messages), allow me to offer a few privacy tips:

- **Limit your friend lists.** Most people assume the more Facebook friends you have, the better. But if your list includes people you know only a little or not at all, you can't think of them as *friends*—you can't trust them to take care of your private data. Everyone has their own rules, but I wouldn't want anyone to be a Facebook friend who I wouldn't invite into my home for coffee.

  The situation is different with Facebook *followers*, X followers, and other one-way relationships. You may think of these as being more private because you're not required to friend or follow the other person, but that doesn't stop them from reading everything you post about yourself. If you can't control who sees your photos, videos, or updates, censor yourself accordingly.

- **Be careful about what you "like," "favorite," and so on.** When you "like" a post, page, brand, movie, musician, political

candidate, or even a generic category on Facebook, that information is added to your profile—Facebook uses that data to help determine what you're likely to be interested in and therefore what ads to show you. There's a lot of data like that (on Facebook, X, and elsewhere), and you may have to dig deep into each site's settings to find what's being shared and whether or to what extent you can limit it.

- **Don't assume "private" messages really are.** You can send messages in Facebook Messenger that function much like email messages, or have a live chat. You can send direct messages to another user on X that don't appear in your public timeline. And many other social networking sites also offer direct, seemingly private modes of communication with other members. But these messages aren't sacrosanct. Site administrators may be able to read them, and can almost certainly provide them to anyone who showed up with a court order. And there have been cases where, due to a programming error or other security breach, the contents of such discussions have leaked out.

- **Don't assume "secret" services really are.** Lots of services claim to let you share thoughts and feelings with other people anonymously using mobile apps such as Whisper. Unfortunately, as the Wall Street Journal's Geoffrey A. Fowler pointed out in Psst, Secrets You Share Online Aren't Always Safe, such apps can store and transmit enough information about you to give away your identity (and are subject to hacking and bugs, just like everything else). And sometimes, new services that claim to be ultra-secure turn out to be fronts for criminal enterprises…or law enforcement.

- **Limit apps.** On Facebook and other sites that let you install apps, *just say no*. Although each app is different, some of them can read everything you write and spread your data around in ways you might dislike.

- **Use good passwords.** As I said in Choosing Better Passwords and Protect Passwords and Credit Card Info, be sure to use long, random passwords that can't be guessed by human or machine. And, if a site offers two-factor authentication, consider enabling it (see the sidebar About Two-Factor Authentication, earlier). That will greatly

reduce the chance of your account being hacked. Be sure to keep those excellent passwords safe—don't share them, and log out of your user account before letting someone else use your computer.

- **Think carefully about pseudonyms.** You may use an alias rather than your real name on Tumblr, X, or other sites. Although pseudonyms like this can protect your privacy, they're not impenetrable—so again, don't stake anything critical on them. Furthermore, sometimes pseudonymity can work against you, as I describe in the sidebar When Privacy Hurts, earlier.

High-Risk Resources: Social Media

Let me be blunt. If you're at a high risk of being targeted for financial, political, or personal reasons, *you should not use social media at all*. Sign out of all social media websites and apps, don't post anything, and don't sign back in as long as the threat persists. And that goes triple extra for Meta services (Facebook, Instagram, Messenger, Threads).

If you're a celebrity whose brand depends on social media posts, then I'm guessing you have staff who can post things on your behalf—although they, too, may be subject to attacks. In any case, you, personally, should stay as far away from social media as you can if you want to avoid any chance that your activity there, active or passive, could give away your location and other sensitive information about yourself.

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

address for a server, you could end up at a fake but look-alike site designed to steal your password or other personal data.

Several types of DNS attacks exist, including DNS hijacking, which often takes the form of malware that modifies your computer's DNS settings; and DNS spoofing (also known as cache poisoning), which inserts false information directly into a DNS server.

- **ISP monitoring:** As I mentioned in the sidebar Privacy and Your ISP, your ISP can monitor and log any data that flows through its routers—including your IP address and the addresses of any servers you connect to, as well as the quantity and even the content of information that you transfer. These logs may be kept indefinitely and could be seen by your ISP's employees, law enforcement, and (potentially) hackers. Besides monitoring data and perhaps selling it to advertisers, your ISP could censor data—for example, by blocking access to certain domains or the use of certain protocols.

  But, your ISP can't see the contents of encrypted data you send or receive, though it knows how much data was transferred, when it was sent, and who was on each end of the exchange.

- **Router monitoring:** What's true of your ISP is also true of any other router between your ISP and the servers you want to reach, of which there may be many. For example, numerous countries have national firewalls that prevent anyone within their borders from reaching sites or services deemed to be unsuitable. In other countries, government and intelligence agencies may monitor routers, possibly even without their owners' knowledge (see Big Brother).

- **Malware:** If you have the misfortune to download a virus, worm, Trojan horse, or other malware, any number of privacy risks could exist. Some malware logs every keystroke that you type in order to capture passwords, credit card numbers, and other personal data. Other malware may alter your DNS settings (as described earlier in this list), turn your computer into a spam-sending robot, display an endless series of pop-up ads, or encrypt all your data and demand ransom payment.

- **Location discovery:** I've mentioned how your IP address can give away your location and sometimes even your identity—and your IP address is known to every site and service you connect to. Even if you use methods (discussed ahead in Prevent Snooping) to disguise your IP address, your device may determine and transmit your location using other methods, including the names of nearby Wi-Fi networks, triangulating on cellular radio signals, and using GPS coordinates (for suitably equipped devices).

Pretty grim, right? Could be, but fortunately, many of these privacy threats are easily overcome, as I explain in the rest of this chapter.

Quantum Computing and Encryption

Nearly all of the world's cybersecurity infrastructure is predicated on the assumption that suitably strong encryption, supported by suitably strong passwords, is generally safe from brute-force attacks (in which the attacker essentially tries every possible password or encryption key until the right one is found). The sheer number of possible combinations makes it incredibly unlikely that the encryption could be cracked in your lifetime…given conventional computing technology.

But governments and large corporations have, for years, been working on an entirely new technology—quantum computing—that could change the rules entirely. On the plus side, quantum computing promises new forms of encrypted communication that are theoretically unbreakable and impossible to eavesdrop on. However, the same technology could enable a quantum computer to crack traditional strong encryption in seconds rather than millennia by, roughly speaking, trying every possible solution at once. In essence, such a computer could invalidate virtually all modern digital security systems.

One day, perhaps not long from now, we (and the companies that make the devices and software we all depend on) are going to have to find a way to adapt to that new reality. Work is well underway; Apple, for example, has already added "post-quantum" encryption to iMessage. But you should be aware that there could soon come a period during which the encryption tools we've depended on for so long are insufficiently strong to fend of quantum attacks. For more, read NSA seeks to build quantum computer that could crack most types of encryption in the Washington Post.

Prevent Snooping

If you take steps to secure the connection between your computer (or other devices) and the internet, you eliminate one of the easiest methods available to an attacker who might want access to your private data—or who might be searching randomly for low-hanging fruit. Depending on your situation, you may use any or all of several techniques.

Note: In later chapters, I'll talk specifically about additional steps you can take to Browse the Web Privately and Improve Email Privacy, among other things.

Here are some of the ways you can keep outsiders from snooping on your internet connection.

Encrypt Your Wi-Fi Connection

Even if your main computer uses a wired Ethernet connection, you're bound to have some device—a laptop, smartphone, tablet, smart speaker, or streaming media device, for instance—that can connect only using Wi-Fi. Without any encryption at all, your internet connection might look something like **Figure 6**.

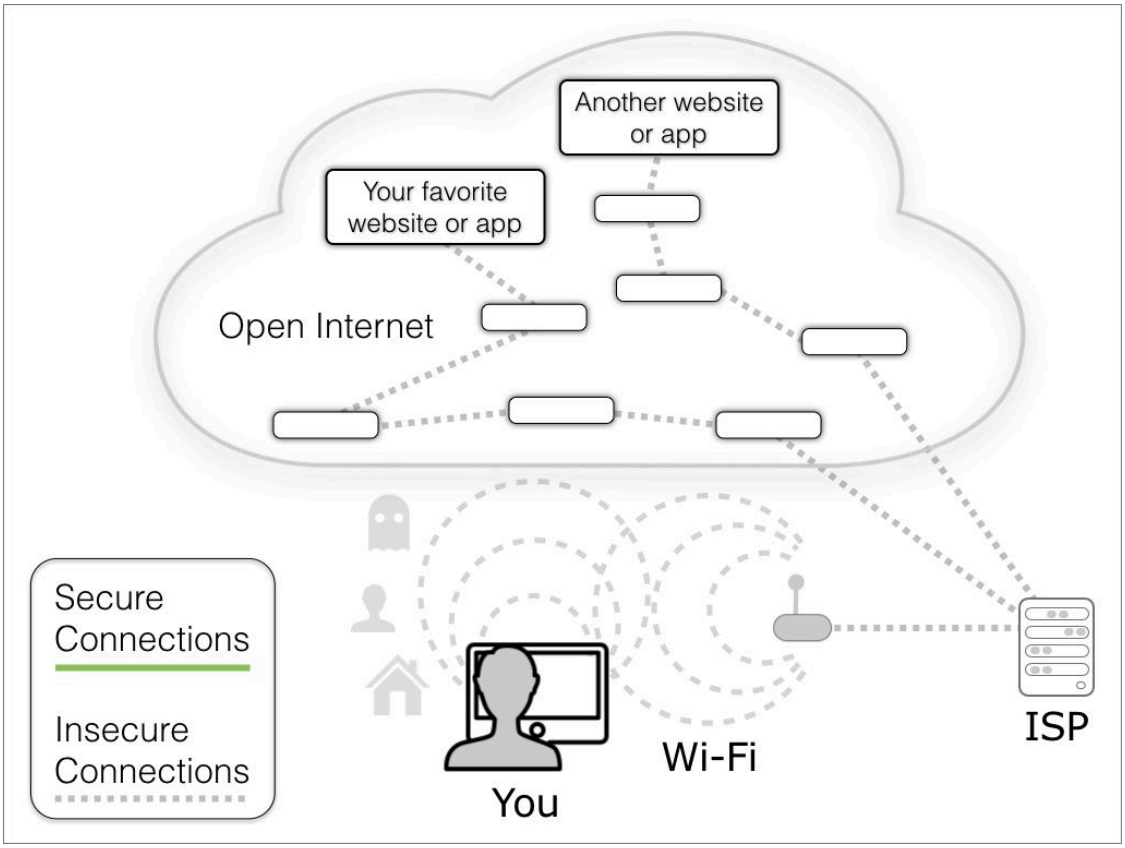


Figure 6: Without encryption, your Wi-Fi connection—the most local and most vulnerable portion of the path to other computers on the internet—could easily be "sniffed" by someone nearby. In this example, *no* connections are secure.

Assuming you own or control the Wi-Fi router, you should take immediate action to make certain no one else can eavesdrop on your Wi-Fi communications—see the documentation that came with your router or refer to the manufacturer's website for instructions:

- **Use WPA.** Wi-Fi Protected Access (WPA) is the most secure standard for Wi-Fi encryption currently in widespread use. It comes in several flavors, so you may see options like "WPA3," "WPA2 Personal", "WPA2-PSK [AES]" and "WPA-PSK [TKIP] + WPA2-PSK [AES]" (**Figure 7**). I can't give exact configuration details here, because every router is different, but if the manufacturer's instructions are insufficient, you can find lots of good information in Glenn Fleishman's ebook *Take Control of Wi-Fi Networking and Security*.

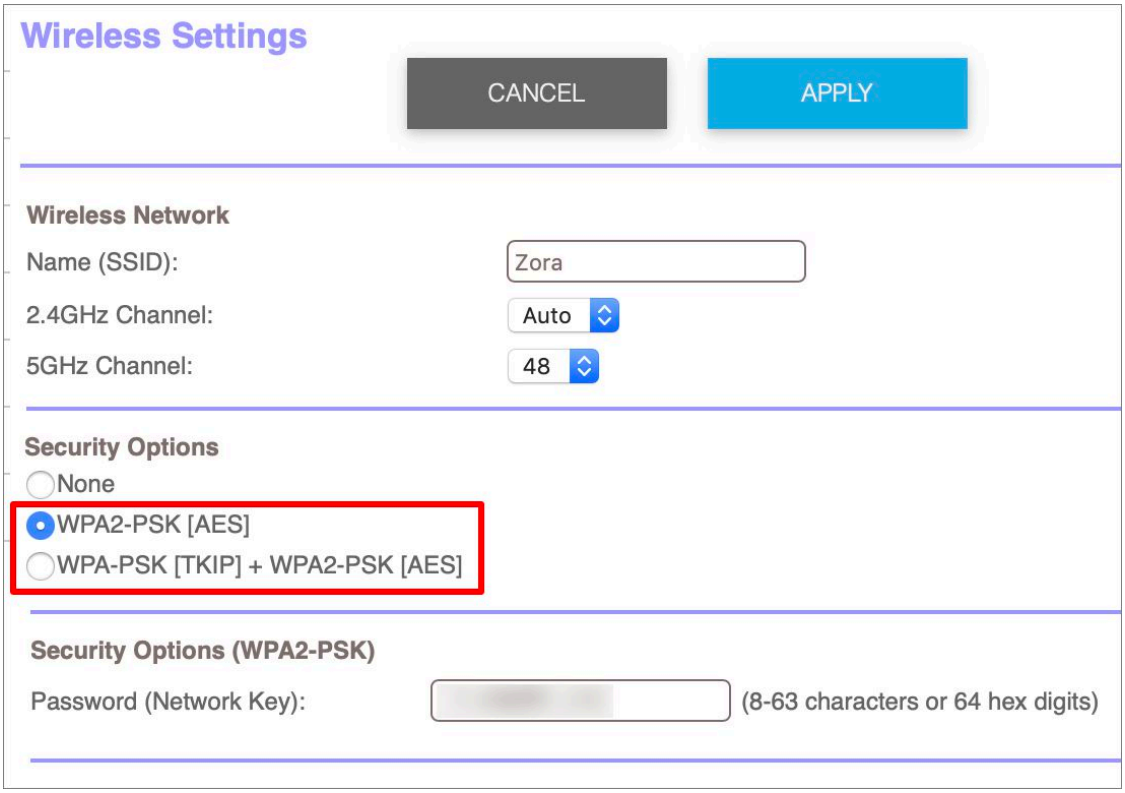


Figure 7: Wireless security options for a Netgear Orbi wireless router. Choose any option that includes "WPA" (outlined in red) and you should be fine.

As I mentioned earlier, although WPA is vastly more secure than its predecessor, WEP (Wired Equivalency Protocol), WPA2—the version that's been in use since the mid-2000s—has vulnerabilities that could enable an attacker to see your data, while WPA3, which addresses those issues, is available on many newer devices, and it even encrypts wireless traffic if you don't set a password. Unfortunately, WPA3 also contains several vulnerabilities, which individual device vendors may or may not have patched. Even so, all things being equal, you should use the most recent version of WPA available to you, and no matter what you do, *do not skip wireless encryption*. You could choose "None" as the wireless encryption type, but don't; that's ridiculously insecure and never the right choice if you can avoid it.

Note: If WEP is the only option available on your Wi-Fi router, it's probably very old. Now is a good time to think about replacing it.

With WPA-encrypted Wi-Fi, your connection looks like **Figure 8**.

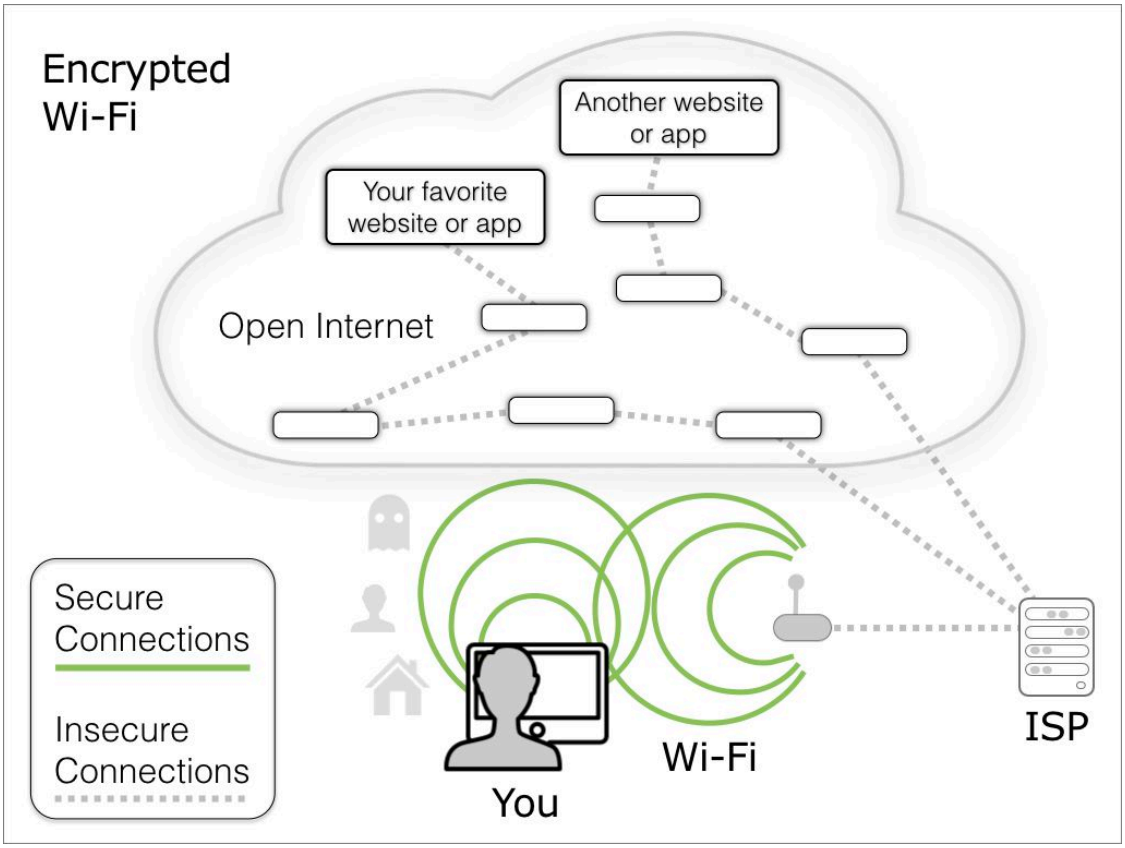


Figure 8: With encrypted Wi-Fi, you protect the local portion of your internet connection from casual sniffing, keeping in mind that even WPA2 is not immune to hacking.

- **Use a good wireless network password.** The password you create to connect to the Wi-Fi network should be long, random, and complex to avoid automated attacks in which a computer systematically tries likely passwords until it finds the right one.
- **Use a good administrative password.** In addition to the password for your wireless network, your Wi-Fi router has an administrative password, which you must enter in order to modify its settings. Be sure to change the default password—it's often "password" or something else similarly insecure. Ideally, the administrative password should be different from, but just as strong as, the password for your wireless network.

Tip: See the sidebar Choosing Better Passwords for advice on creating a strong password.

What if you're on someone else's Wi-Fi network? If it happens to use WPA, that's good, but not perfect—and since other people will know

the password, your connection is somewhat more vulnerable to hacking than your own network would be. (It's still *way* more secure than a network that uses no encryption at all, though, so if you run a public network, don't be bashful about turning on encryption and posting the password all over the place.) If the network uses no encryption or WEP—or if you want extra insurance on a public WPA network, which you probably should—you need to take matters into your own hands by using a VPN, as I describe next.

Note: Even without encrypted Wi-Fi, you can and should use encrypted connections to specific services, such as web and email servers (see Browse the Web Privately and Improve Email Privacy, respectively). But even if your connection to a certain server is encrypted, your device may still send and receive loads of other, unencrypted data. That's why it's always wise to use encrypted Wi-Fi.

Use a VPN

A *virtual private network,* or VPN, is a special type of network connection that encrypts all the internet traffic flowing between your device and a VPN server somewhere on the internet.

Think of a VPN as a tunnel running through your physical (Wi-Fi, cellular, or wired) internet connection that's impenetrable from the outside but open on both ends (**Figure 9**). Since VPNs encrypt everything, they even make it safe to use an unencrypted Wi-Fi connection.

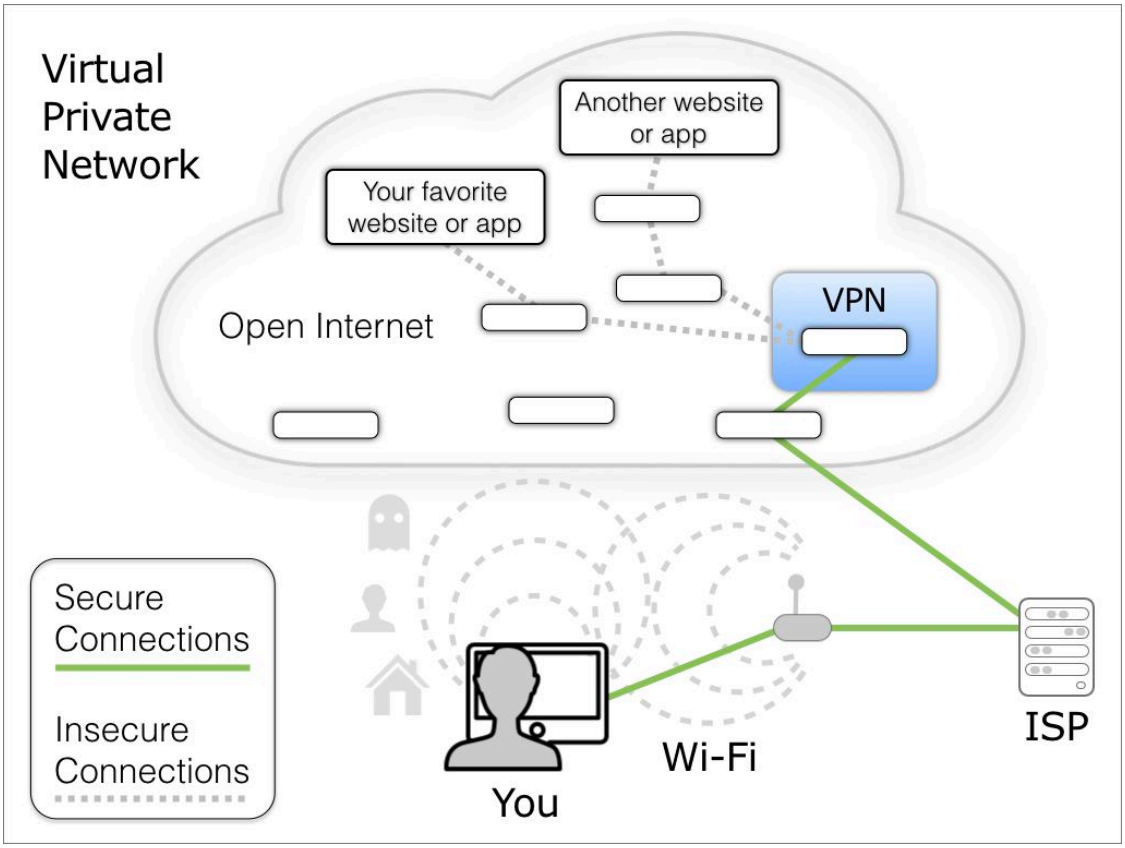


Figure 9: Using a VPN encrypts the entire internet connection between your device and your VPN provider, protecting a greater portion of your data's path than encrypted Wi-Fi alone.

With a VPN, your computer or other device appears to be on the same local network as the VPN server. So, for example, if that server is located in your employer's data center, connecting to it gives your computer the same access to your corporate network that it would have if it were in the same building—access that would otherwise be blocked from the outside by a firewall. And your IP address will be assigned by the VPN, so if the VPN server is in, say, France but you're physically in Los Angeles, your IP address will most likely appear (from the perspective of any server you connect to) to be in France.

Organizations with remote workers or multiple locations often run their own VPNs, and if you work for such a company, your IT people can explain how to get up and running. But ordinary citizens can also take advantage of VPNs by signing up for any of numerous commercial services. Some of them work with your existing operating system and simply provide instructions for configuring your settings, but most of

them provide their own free software that requires little more than entering your username and password.

VPNs are certainly useful in some situations, but even as they have become more popular and mainstream, my own thoughts about them (and recommendations by security professionals) have shifted in recent years. The problems with VPNs may outweigh their benefits, and even when a VPN is the correct choice, *which* VPN you use can make the difference between increasing your privacy and greatly diminishing it. Here are some factors to consider:

- **Other layers of encryption:** If you're connected to an open, unencrypted Wi-Fi network *and* visiting websites without TLS/SSL (that is, with URLs that start with `http://` instead of `https://`) or connecting to email servers that don't offer TLS connections, then yes, having the security that a VPN's encryption provides would be valuable. Except…most modern Wi-Fi networks, web servers, and email servers *do* encrypt the data they send and receive already, so you likely have at least one and probably two layers of encryption protecting your most important online communication. That means—for most people, in most situations—a VPN is superfluous.

What Are TLS and SSL?

Websites, email servers, and other internet services often use a protocol called TLS (Transport Layer Security) to encrypt the connection between the client (your app or device) and the server. It's a updated and more secure version of an older protocol called SSL (Secure Sockets Layer).

Even though TLS has been around since 1999, by long habit, many sites and companies still use the older SSL terminology, and the certificates that enable TLS are still commonly called SSL certificates. Because both terms are still widely used, I generally say "TLS/SSL" in this book.

- **Limits to a VPN's protection:** As I described above, a VPN protects data in transit *only* between your device and the VPN server (sometimes called an *endpoint* or *exit node*) on the other end. Anything between that server and your final destination may not be

encrypted, so there are still ways an attacker could intercept your communication during part of its journey. In addition, whatever site or service you connect to will still be able to see what you do and in many cases figure out who you are, even if your IP address is obscured, because of other clues your device provides (such as cookies and browser fingerprinting, both discussed later). Remember, security is not anonymity (refer back to Privacy vs. Security vs. Anonymity).

- **Logging and tracking:** Many VPN providers claim not to keep logs—which, if true, is a good thing, because it means that no one could later figure out what you did while connected to the VPN by examining those logs. But companies sometimes fib. This story, for example, describes an incident in which detailed logs were leaked from a VPN operator that claimed not to keep any logs.

  Even if a VPN provider doesn't keep logs of what you do while connected, they may still track your activities in other ways, often to make money from ads. What you must keep in mind when using a VPN is that *the VPN provider, by definition, has access to all the data you send and receive while connected*. If that data isn't already encrypted in some way, in theory, it could be seen and used by the VPN service. On the other hand, per the first bullet above, if the data is encrypted anyway, there may be little point to using a VPN in the first place.

Note: Nearly always, when you connect to a VPN, your DNS lookups are handled by the VPN's DNS servers, even in you specified different servers in your network settings (see Avoid DNS Mischief). That means your DNS lookups while connected to a VPN are at least theoretically subject to tracking.

- **VPN server location:** Are your VPN's servers really where they say they are? Most VPN services let you choose the country or region you connect to. But where they *say* you're connecting to and where you're really connecting to may not match! For example, quite a few customers have asked us why they were being charged in euros for their purchases even though they're in the United States.

It turned out that most of them were using NordVPN, and even though they chose a server in the United States, NordVPN actually connected them to servers in Europe! (The reverse has also happened.) I've seen this with other VPNs, too. To know for sure where you've connected, check it yourself. While using your VPN, visit an IP address geolocation site such as IP Location, which will tell you (in general terms) where your public IP address is geographically located.

Note: This apparent bug doesn't imply threats to your privacy or security; it merely reinforces the sound advice to "trust but verify."

- **Website compatibility:** For a variety of reasons, some websites simply don't work properly when you connect to them via a VPN. This is especially true when you choose a VPN server in a different country, as many sites behave differently depending on the visitor's perceived location. (And, if you're using a VPN specifically to access streaming media unavailable in the country where you live, you should be aware that many streaming services go out of their way to identify and block connections from VPNs.)
- **Manual connection:** In general, VPNs are active only when you explicitly turn them on. If your device goes to sleep, switches physical networks, or loses its connection, you may have to manually restart the VPN. Even when you stay on the same physical network, VPN connections can flake out—sometimes without any obvious sign that you've lost your secure connection—just when you need them most.
- **Speed:** Because of the overhead required to encrypt and decrypt data, VPNs are always slower than unencrypted connections. Whether that's noticeable depends on your hardware, software, VPN type, and the location of the server you connect to. But it could cause problems for activities that require lots of bandwidth or low latency, such as streaming 4K video or fast-paced games.
- **Per-device connection:** Usually, a VPN connection must be made individually from each device—and you may have devices

(such as smart speakers) that can't use VPNs. There is a solution to this problem, however: Consider a VPN Router or Privacy Appliance, discussed ahead. I used one of these myself for a few years. But (per the previous point) they can cause internet access for your entire network to be considerably slower and laggier.

- **Cost:** It costs money for a company to provide VPN services, and usually that cost is passed directly on to consumers. (How much you pay per month or year varies widely with the provider, as speed, security, and other features tend to correlate with price.) So, if a VPN service is free, I become suspicious that the provider is using my data in some sneaky way to pay their bills—and if it's "free, ad-supported," I run away as far and as fast as I can, since they've come out and told me they're going to track my usage to serve me ads.

Note: If you're an Apple user with a paid iCloud+ subscription, you have access to a *VPN-like* service called Private Relay, which may be adequate for your needs. See iCloud Private Relay for details.

- **Trustworthiness:** I've left the most important consideration for last. Can you actually trust your VPN provider, a company that can see all the data you send and receive while connected?

  Here's a cautionary tale. Between 2017 and 2021, a company originally known as Crossrider (later rebranded to Kape Technologies) began buying up VPN providers, including ExpressVPN, Private Internet Access (PIA), and CyberGhost. Crossrider was associated with some seriously shady business activities. Some sources accused the company of creating malware, while others more charitably said they merely created a software platform that some bad actors misused to distribute malware and inject ads into internet content. In any case, it raises warning flags.

  Kape claims to have shut down that platform and replaced its leadership, which may be true. However, the company owns not only several VPNs but also several *VPN review sites*, which—surprise!—rank their own services at the top. (See the sidebar Beware VPN Review Sites, ahead.) Whatever else can be said of the compa-

ny or their VPN services, running review sites that favor their own products is still bad news; it tells me that the company is simply not trustworthy. It's for that reason that I no longer use or recommend PIA (my former top pick) or ExpressVPN.

- **Undisclosed vulnerabilities:** A May 2024 article in Ars Technica, Novel attack against virtually all VPN apps neuters their entire purpose, describes a method that could enable an attacker to secretly reroute data that *appears* to be going through a VPN through an insecure path that would enable them to snoop on (or even alter) the unencrypted traffic. That attack would require someone to infiltrate the local network to which your devices connect (unlikely to be a problem with a home network, but potentially a concern with business and public networks), and it reportedly doesn't affect Linux or Android devices. Even if such an exploit were used on your network, it wouldn't let the attacker see the contents of data encrypted in other ways (such as visiting an HTTPS website or using an email account that connects via TLS/SSL), and I presume that companies like Apple, Google, and Microsoft are already hard at work on a fix. Be that as it may, there could still be other bugs or flaws in VPN software that would lead to the appearance that your data is protected when it really isn't.

I want to reiterate that, despite all these issues, a VPN is still an excellent idea in certain situations—for example:

- You're living or traveling in a country known to monitor or censor internet data.
- You have to use websites or email servers that don't offer encrypted connections.
- You have a specific reason not to trust your ISP (see the sidebar Privacy and Your ISP) and you want to prevent them from seeing what you do online.
- You're a journalist, crime victim, celebrity, zillionaire, or someone else who might be targeted for surveillance, and you want to take every possible precaution.

- You run a book publishing business in Canada but you frequently have to look up prices and services on the web as they would appear to a visitor from the United States or Europe. (I can think of someone offhand who meets this description.)

There are hundreds of VPN providers out there, so how do you pick one? I've tried dozens of VPNs, and my personal choice shifts periodically. At the moment, I'm using Proton VPN; it has worked well for my needs, the price is reasonable (especially when bundled with other Proton services), I consider the company reputable, and it's subject to strict Swiss privacy laws. But, as with all things related to online privacy, I could learn something at any time that changes my mind.

If, for whatever reason, Proton VPN doesn't float your boat, here are a few other alternatives that strike me as trustworthy:

- Bitdefender VPN
- IVPN
- Malwarebytes Privacy VPN
- Mullvad VPN
- NordVPN (but see the "VPN server location" bullet a few pages back)
- WiTopia

Tip: The Opera browser for macOS and Windows includes a free, built-in VPN. It works only within Opera, but a paid version, VPN Pro, protects your entire internet connection.

You may find another VPN you like better for some reason. That's fine; just keep in mind the factors I've mentioned. But please don't write to ask me "What about *this* VPN provider?" or "Now that six months have passed since the last time you updated your book, which provider are you using now?" I get…a lot of email like that. There is no perfect, complete, or definitive reference for VPNs, and life is too short to review every single one that comes along. All I can say is: do your homework and keep your eyes open.

Beware VPN Review Sites

If you were to search the web for reviews of VPN services—but please don't; I'll explain why in a moment—you would find page after page of search results pointing to VPN review sites. Sites like this, to put it as delicately and generously as possible, are teeming cesspools of greed and lies, representing some of the very worst elements on the internet. They appear to offer objective comparisons and recommendations of VPN services, but more often than not, appearances are extraordinarily deceiving. (There *are* reputable VPN reviews out there, from well-known sites such as Wirecutter and Wired, but I'm speaking here of one-off sites with no pedigree.)

As I mentioned, some VPN companies host their own review sites, which rank their own products at the top. But even independent sites have rankings skewed by providers' affiliate programs. Because of the bloodthirsty nature of competition among VPN providers, they're constantly trying to outdo each other with ever-increasing affiliate fees for referred sales. This competition—along with policies that ignore or even encourage spamming and other untoward marketing tactics—has led to a cottage industry of sites whose recommendations are based *solely* on how much they believe they can make from affiliate fees, facts be damned. VPN services that offer lower affiliate rates appear lower (if at all) in the rankings, and services that offer more appear at the top, even if they're dodgy, fly-by-night providers.

I'm ashamed to say that I unwittingly contributed to this mess. A company hired me to write an elaborate, detailed comparison of VPN providers, and as far as I could tell, the firm in question was reputable. So I spent weeks doing careful research and testing, putting my best work into developing recommendations that would, once and for all, provide objective data on VPN providers.

But when my review was finally posted, it appeared on a completely different site, with my byline removed and some of the wording changed in truly bizarre ways. Most significantly, though, my top recommendations were replaced with entirely different providers that I had, in fact, ruled out. Even more egregious, the site left my actual numeric test results in a comparison table but swapped out the names of the real providers for the ones they wanted to push.

So, a word to the wise: don't believe anything you read on VPN review sites, even if it sounds like I might have written it!

Consider a VPN Router or Privacy Appliance

VPN software running on a computer or mobile device protects only that device. If you have lots of devices in your home or office—and especially if some of them (like NAS devices, smart TVs, and streaming boxes) can't run VPN software themselves—you may want to approach the problem in a different way. Instead of making a VPN connection from each device individually, use a special router to make a permanent connection to your VPN provider, and then connect all your other devices (via Wi-Fi or Ethernet) to that router.

Consumer-grade VPN routers of the type I'm referring to range in price from roughly $200 to $600 plus the cost of a VPN subscription. (That assumes the routers offer Wi-Fi; Ethernet-only VPN routers are often less expensive.) You plug one of these into your broadband modem, configure it with the account credentials for your VPN provider, and then switch all your devices to connect to the local network created by the VPN router. Then, like magic, all your internet traffic is protected by the VPN.

Sometimes you can buy a preconfigured VPN router from your VPN provider—for example, I used a CloakBox Pro VPN Router from WiTopia for a number of years. Alternatively, you can find out from your provider which router models they support and then either buy a preconfigured router for that service from a third party or (if you have sufficient geek skills) download and flash the router firmware for the proper provider yourself. For a wide selection of VPN routers that work with many popular VPN providers, visit FlashRouters.

A closely related category of device is what I refer to as a privacy appliance. It's typically a standalone box that functions as a VPN router but also offers a network-wide firewall, ad blocking (see Block Ads), and other privacy features. Here are a few random examples:

- Deeper routers
- Firewalla (numerous models)

- InvizBox

Note: If your main concern is blocking ads, you can also install the free Pi-hole software on an inexpensive Raspberry Pi single-board computer or on devices running any of numerous Linux distributions. A Pi-hole can optionally connect to a third-party VPN, too (at additional cost).

My caution about using all such devices, and especially the privacy appliances that go beyond a simple VPN router, is that network-level VPNs, filtering, and blocking can work against you. You may encounter sites that block VPN traffic, or webpages that don't load, and convincing your router to adjust VPN settings or selectively turn off ad blocking to address a problem like this can be an exercise in frustration. (You may be able to work around some such issues with a dual router or dual gateway setup that lets you segregate VPN-protected traffic from unprotected traffic on your network; another term for this setup is "split tunneling.") Also keep in mind that a VPN router or privacy appliance can't protect your computer or mobile device once it's no longer in reach of your home network. In those cases, you'll need either software solutions or an additional mobile privacy device you carry with you.

Use TLS/SSL If Possible

Whenever possible, use encrypted connections to the servers you visit. For websites, that means preferring sites that use HTTPS (discussed in What About HTTPS?); for email servers, that means using TLS/SSL (see What Are TLS and SSL?); for remote terminal sessions, it means using SSH instead of Telnet; for file transfer, it means using SFTP, FTPS, or WebDAV HTTPS instead of FTP. All these types of communication offer end-to-end encryption between your device and the remote server, whether or not your internet connection is encrypted in other ways (**Figure 10**). That limits your potential privacy exposure considerably.

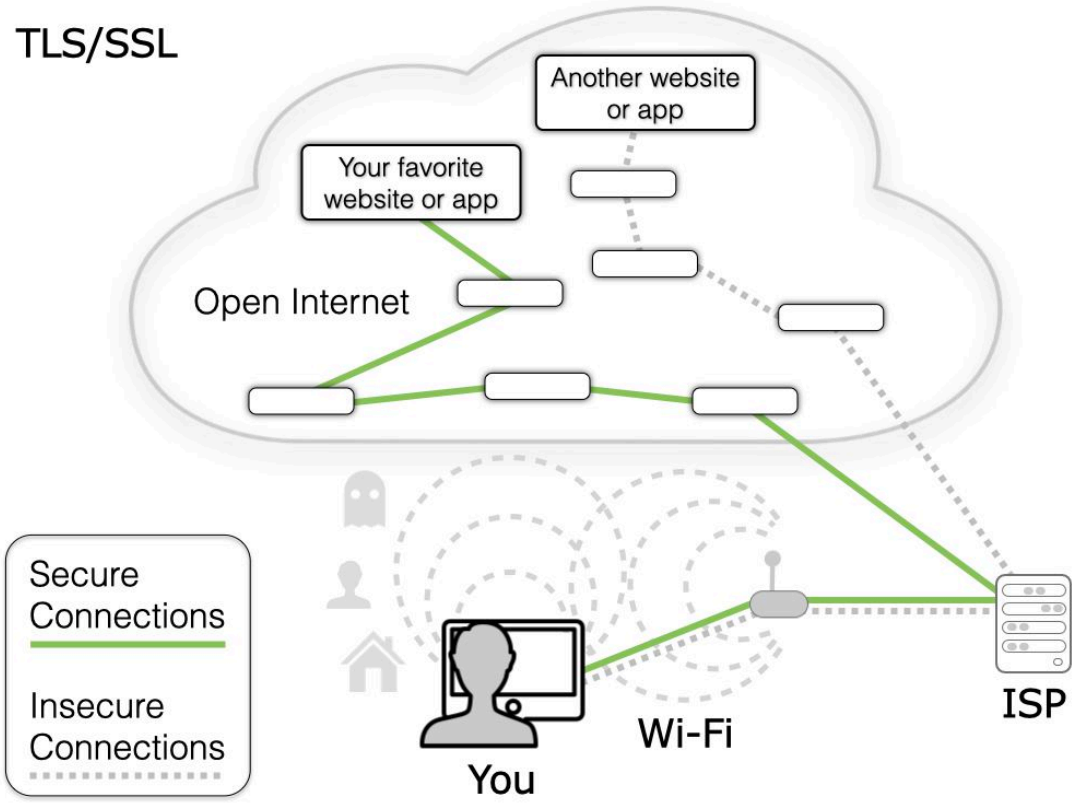


Figure 10: Using TLS/SSL encrypts an entire communications channel between your device and a particular remote service. But other insecure connections may be active at the same time.

Because TLS/SSL has become vastly more common in the past decade, especially for websites and email, you're more likely than not to have encrypted browsing sessions by default, which in turn means those connections are protected even over unencrypted Wi-Fi connections.

TLS/SSL Implementation Bugs and Issues

Although using TLS/SSL is much better than not using it, numerous bugs and vulnerabilities have been found in various TLS/SSL implementations over the years (and some may even have been planted deliberately to facilitate government surveillance). They're usually fixed promptly, but there could always be undiscovered issues.

Sometimes a certificate authority (a company that issues SSL certificates to others) can also screw up, for example by issuing fraudulent certificates to impostor companies. You can't prevent this, but it's a reminder that the system is inherently imperfect.

Avoid DNS Mischief

I mentioned threats such as DNS hijacking and DNS spoofing that can lead you to a server that looks real but is only impersonating (inserver-ating?) the one you want to reach. How can you prevent this?

Use a Better DNS Provider

The best place to start is to *change your DNS provider*. Your ISP provides DNS services automatically, but you're free to connect to other DNS servers if you like. Some third-party DNS servers offer much better performance than your typical local ISP, and if you choose one with a good security reputation, you'll reduce the risk of DNS mischief too. There are quite a few good (and free) choices. Keep in mind, however, that whatever DNS provider you use—whether it's your ISP or a third party like the ones listed here—that company will have access to all the domain names your devices look up, so you should think carefully about the trustworthiness of any such company.

Here are my suggestions, starting with my current favorite. In each case, follow the link for detailed configuration instructions, but the short version is: change the DNS servers on each of your devices to the addresses listed below:

- **1.1.1.1:** This service by CloudFlare is noteworthy for its speed and privacy, and all DNS lookups are encrypted. Use DNS addresses `1.1.1.1` and `1.0.0.1` (IPv4); `2606:4700:4700::1111` and `2606:4700:4700::1001` (IPv6).
- **Quad9:** Quad9 not only provides DNS services but also helps block unsafe websites (such as those distributing malware). Use DNS addresses `9.9.9.9` and `149.112.112.112` (IPv4); `2620:fe::fe` and `2620:fe::9` (IPv6).
- **OpenDNS:** I used OpenDNS from Cisco for years and still like it, but I prefer the business model and features of the services above. Use DNS addresses `208.67.222.222` and `208.67.220.220`.
- **Google Public DNS:** Yes, Google has its own DNS service too! It's fast and reliable, and Google claims the service isn't used to collect

private data or serve ads. Is that true? I don't know. Use DNS addresses `8.8.8.8` and `8.8.4.4`.

There's also free software, originally developed by OpenDNS, called DNScrypt, that *encrypts* and authenticates all your DNS requests (to any compatible DNS provider, including most of the above), thus acting as an additional defense against DNS spoofing and man-in-the-middle attacks. This page lists a variety of implementations of the software for various platforms.

Use an Enhanced DNS Provider

The services above give you fast, reliable DNS lookups that are arguably more secure and private than what your ISP offers. But some DNS providers go a step or two further. For example, these two companies offer DNS services that also block most ads and trackers by filtering out requests to domains known to be used for such purposes:

- NextDNS: You must sign up for a free account, but thereafter you can use the service in a basic way by adjusting your DNS settings, or add more capabilities (and simpler configuration) by installing an app. You can get 300,000 monthly DNS lookups for free; paid plans with unlimited lookups cost $1.99 per month or $19.90 per year.
- AdGuard DNS: AdGuard offers free, public DNS servers that also block many ads; use DNS addresses `94.140.14.14` and `94.140.14.15` (IPv4) and `2a10:50c0::bad1:ff` and `2a10:50c0::bad2:ff` (IPv6); apps are also available. The company also offers private DNS servers with terms similar to NextDNS: 300,000 monthly DNS lookups for free or unlimited lookups for $19.99 per year. (The private DNS services are also included with paid AdGuard VPN plans.)

Note: CloudFlare, the company behind 1.1.1.1, also offers an app called WARP, which incorporates the fast, encrypted DNS lookups of 1.1.1.1 into a VPN-like service that also claims to speed up browsing.

Another way to get both improved DNS service and network-level ad blocking is to use a separate device on your network for this purpose; see Consider a VPN Router or Privacy Appliance, a few pages back.

Avoid Malware

Recent versions of macOS and Windows are highly resistant to malware (including such troublesome variants as ransomware and scareware), especially if you keep up to date with all security updates, turn on the built-in firewalls, and don't disable any built-in security features. If you practice common sense—don't click links in email, chat, or other messages when you aren't absolutely certain of the message's authenticity, don't download pirated movies and suspicious software, stay away from sketchy websites, and so on—you have a reasonably good chance of avoiding viruses, worms, and other nasty programs that could compromise your privacy.

Installing third-party antivirus software, of which (as I'm sure you're aware) there are a gazillion choices, will improve your odds even more. However, I urge you not to put your entire trust in any anti-malware program. Even the best ones aren't perfect, and malware authors are always finding clever ways to defeat them, and antivirus software can deliver false positives and even *cause* problems on your devices. You still need to compute with both eyes open.

Previously, my advice was that third-party anti-malware software was a must on Windows, but unnecessary for most Mac users. Given the evolving nature of both of these operating systems and the outside threats they face, I'm currently more inclined to say the following:

- **Windows:** If you use an up-to-date installation of Windows 11, the built-in Windows Defender software—as long as it's enabled, with "Real-time protection" and "Cloud-delivered protection" turned on—should be adequate protection for most users. If your version of Windows is older, or if you engage in risky online activities, you should consider adding a third-party anti-malware tool.
- **macOS:** Mac security experts are saying that the malware threat is bigger than it used to be, and that Apple's built-in tools, while pretty good, aren't quite up to the job. So unless you're a sophisticated user with a strong spider-sense about potential dangers (and good backups), a third-party anti-malware app is not a bad idea. Two such apps worth looking at are ClamXAV and Malwarebytes.

Anti-malware is less crucial on mobile devices—and is almost irrelevant on iOS/iPadOS, as Apple's security measures make it nearly impossible for third-party anti-malware apps to access the parts of the system where malware could operate. (Android anti-malware apps, meanwhile, are often fraudulent—buyer beware.)

What About Adware?

I'd like to say a few words about a variety of malware known as adware—and its cousin, spyware. *Adware* (as the name suggests) pops up ads on your computer—sometimes even when you're not in a web browser, and even if you've blocked pop-up windows or installed ad-blocking browser extensions. *Spyware* tracks what you do and where you go, and may also capture information like passwords and credit card numbers. Adware and spyware often go together.

What's interesting about adware is that you could easily install it yourself without realizing that's what you're doing! A slimy practice that I'm seeing more often is when a download site takes perfectly good software from someone else and wraps it in a custom installer that also puts adware on your Mac or PC.

Here's how to protect yourself:

- Avoid software download sites like CNET's download.com. Always download software directly from the developer; for Mac users, the Mac App Store is an even safer choice.
- If an installer asks if you want to install any extra software (especially if it's "sponsored") or browser extensions, or make changes to your browser or network settings, say no.
- Avoid installing Java (if you don't have it) or uninstall it (if you do). If you must have Java, deselect any Ask.com or other additional software options in the installer. (For more details on adware bundled with Java on PCs, see Ed Bott's ZDNet article A close look at how Oracle installs deceptive software with Java updates; for what happens on Macs, see Oracle extends its adware bundling to include Java for Macs.)
- If you find you've inadvertently installed adware, follow the MacDailyNews instructions for How to remove unwanted adware that displays pop-up ads and graphics on your Mac, or download Microsoft's Safety Scanner for Windows.

Turn Off Unnecessary Services

Your computer has a number of built-in features that enable other devices to connect to it over the internet—file sharing, screen sharing, printer sharing, location services, Find My, and so on (**Figure 11**). In most cases, these services are good and valuable, and if you actively use them, by all means, keep them turned on.

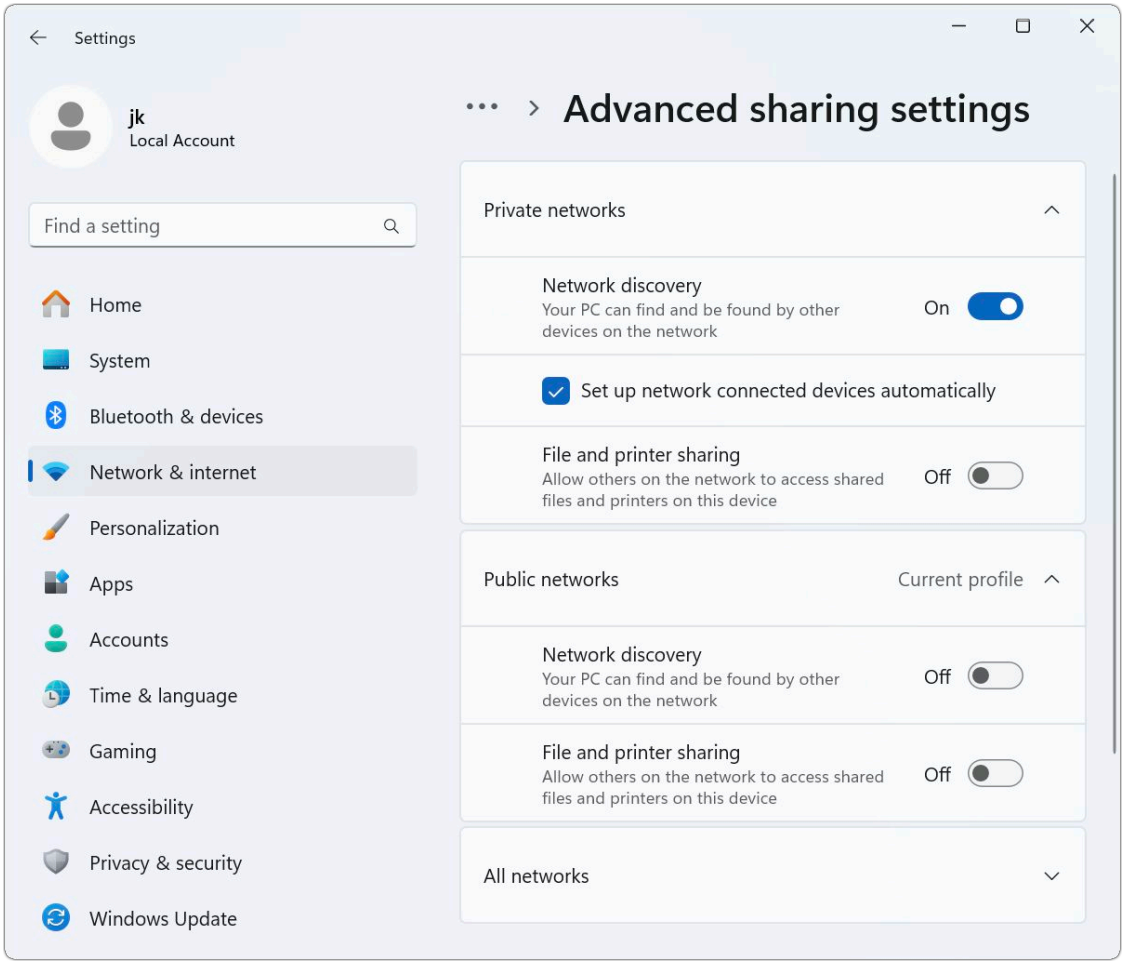


Figure 11: Windows lets you share files, printers, and other resources (as does macOS). Turn off sharing services you don't actively use.

However, any service that lets other devices connect to your computer also represents a potential privacy concern (as well as a security concern). What if someone unknown to you guesses your password and connects to your computer without your permission? All sorts of damage could occur.

So, I'll simply give two pieces of advice:

- Turn off any sharing or location services you don't use. (And, if you use a service only rarely, consider leaving it off until it's needed.) On a Mac, look in System Settings > General > Sharing. On a Windows PC, look at Settings > "Network & internet" > "Advanced sharing settings."
- Be sure your computer has an excellent login password. Refer back to the sidebar Choosing Better Passwords.

Note: For other devices that connect to the internet besides computers, smartphones, and tablets, refer to the chapter Keep the Internet of Things Private.

Mind Your Camera and Microphone

Most Macs (everything except the Mac mini, Mac Studio, and Mac Pro) and many PCs (especially laptops) have built-in cameras and microphones. I have heard of malware that's designed to spy on you by listening to what your microphone picks up and/or watching what your camera sees. In fact, it's even possible (if rare)—on some PCs, and on very old Macs—for malware to turn on your camera *without* activating the little green LED that normally tells you it's active.

As always, preventing this malware from getting onto your computer in the first place is the best defense. Next best is to use an outbound firewall (see Use an Outbound Firewall, ahead) to catch and block the outgoing data or, on a Mac, an app such as Oversight or Micro Snitch, which alert you whenever your camera or microphone is in use.

In recent years plastic webcam covers have become the latest trendy accessory. A widely circulated photo of Facebook CEO Mark Zuckerberg showed his laptop with a piece of tape over the webcam, and I've heard lots of people saying that's the only safe practice. Conventional wisdom seems to be saying that (a) malware that hacks your camera (and its light) is ubiquitous and unavoidable; (b) if you don't physically block your camera, the bad guys will definitely see you naked.

Except…none of that is true. Malware of this type is both uncommon and avoidable. (Modern Macs, in particular, can't be hacked in that manner, and they have hardware lights that show when a camera is in use as well as onscreen indicators for both cameras and microphones.) And, I don't know about you, but given the location of my computers, their cameras would absolutely *never* be able to see anything I'd consider compromising.

I think the whole uproar is much ado about nothing. If it makes you feel better to stick a piece of tape over your camera, knock yourself out, but if you want my professional opinion, it's pointless.

The situation with microphones is a bit different, since microphones don't have lights to let you know they're recording. And odds are better that a microphone would pick up something you wouldn't want strangers to hear than that a camera would pick up something they shouldn't see.

You can turn off your computer's built-in microphone (on a Mac, go to System Settings > Sound > Input and move the Input Volume slider all the way to the left; on Windows, go to Settings > "Privacy & security" > Microphone and turn off "Microphone access"), but software could potentially override this setting without your knowledge (unless you use something like Oversight or Micro Snitch).

Computer manufacturers are beginning to address the underlying issue in hardware. For example, Mac laptops introduced in 2018 or later include either an M-series ("Apple silicon") chip or a T2 security chip that prevents the microphone from being used when the lid is closed—a hardware limitation that malware can't work around.

Use a Firewall

A *firewall* is a program that monitors all *inbound* internet activity and selectively allows or blocks connections based on a series of rules applied to particular ports, protocols, or IP addresses. Firewalls are usually designed to protect your computer from malicious access over

the internet, although they can also censor data and perform a variety of less-helpful activities.

Both macOS and Windows include built-in firewalls; you can activate them with a couple of clicks, and then customize them if you want to allow or block certain types of access. Because these firewalls, with their default settings, are far more likely to help you than to block something useful, I suggest you check to see that yours is turned on right now (**Figure 12** and **Figure 13**). You can find instructions to do this in the Help menu or by using your favorite search engine. For the vast majority of users, sticking with the default settings is just fine.

Note: If your computer uses NAT (as do most computers that connect to the internet via a home broadband router), you already have a certain amount of protection against outside access, but it's not foolproof—and it doesn't hurt to use your computer's firewall too.

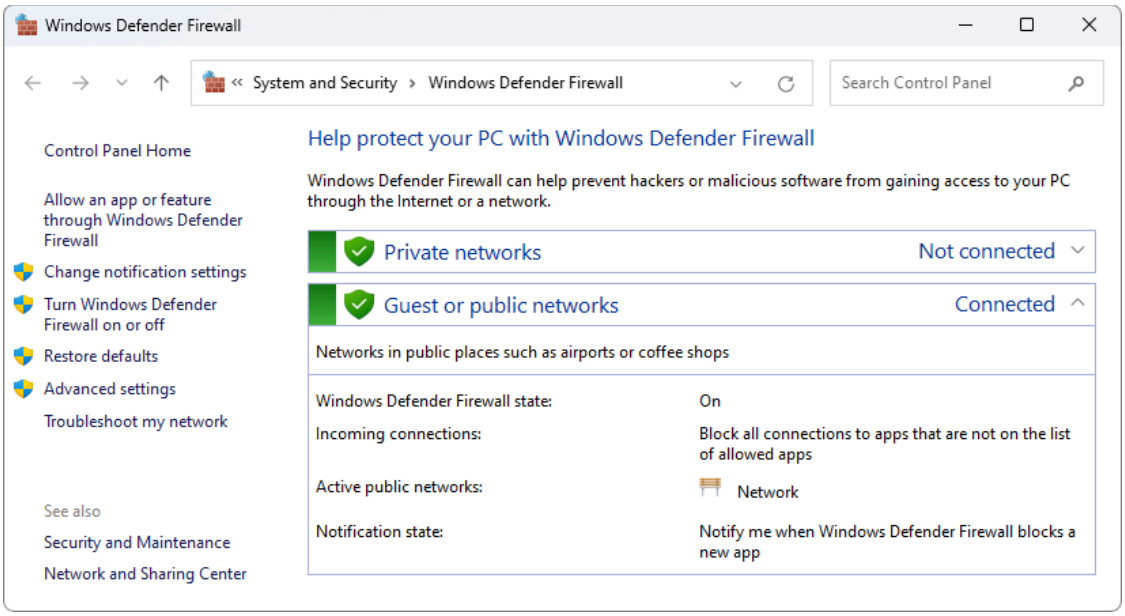


Figure 12: The built-in Windows Defender Firewall in Windows 11.

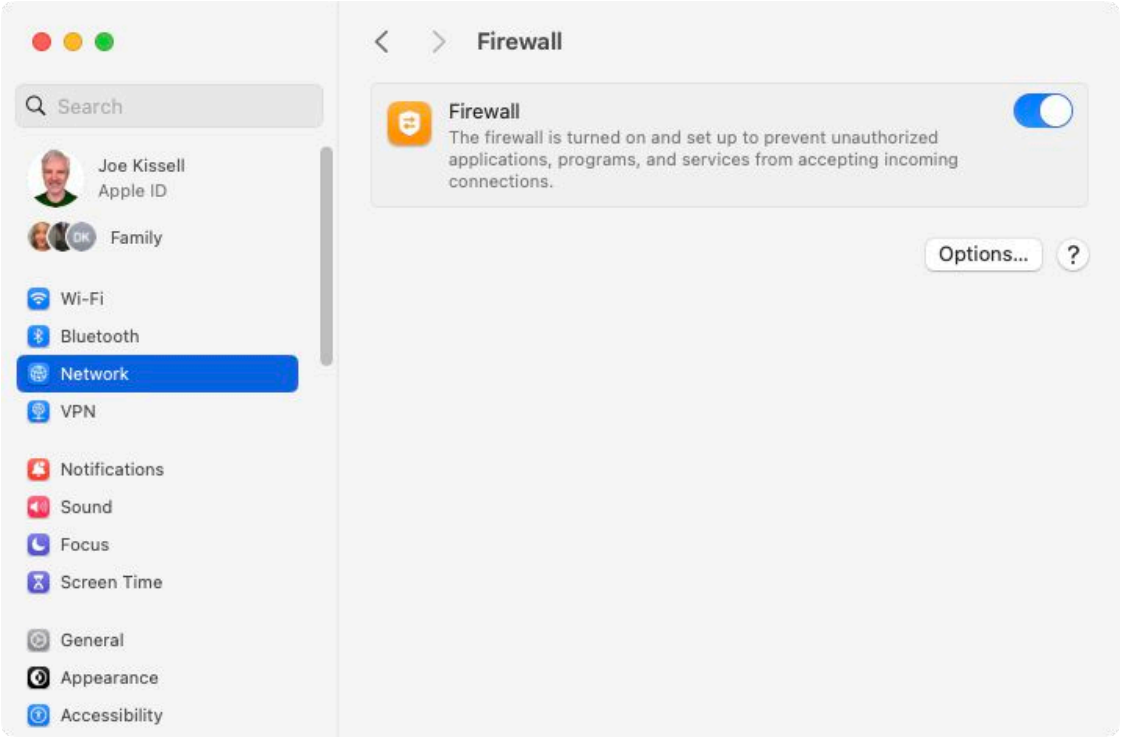


Figure 13: The built-in firewall in macOS.

If for any reason you find your computer's built-in firewall inadequate, you can install any of numerous third-party firewalls instead or in addition. I'll leave that research to you.

Use an Outbound Firewall

I said a moment ago that a firewall monitors inbound internet traffic, which is generally true. However, some firewalls monitor *outbound* traffic (instead of, or in addition to, incoming traffic). The main reason is to make you aware of—and enable you to block—software that might be sending out private information invisibly in the background.

Lots of software connects to the internet without a visible interface, and it's nearly always perfectly legitimate. Your email app downloads your messages in the background, many apps check periodically for software updates, Dropbox syncs newly changed files, and so on. These activities are fine, but if you downloaded malware that secretly logs your keystrokes and tries to connect to a server somewhere to send them to an attacker, that's a problem. And, while some software "phones home" to validate licenses or send registration data, un-

scrupulous developers have been known to collect and send personally identifiable information without users' consent.

I've tried a few outbound firewalls, and I'll be the first to admit that they're annoying—given default settings, they're constantly popping up alerts about outgoing connections, most of which are innocuous but all of which (thanks to the firewall!) now require attention. (To be fair, you can approve any outgoing connection so you're interrupted only the first time it appears—but I still find this happens often enough to be irritating.) They also tend to induce paranoia by making everything look scary. But if you are worried about data being sent from your computer without your knowledge—or just want to understand more about those invisible connections—you might want to give one a try.

On macOS, the best-known outbound firewalls are Little Snitch and Lulu. There's also an app called Murus that is both an inbound and outbound firewall. On Windows, you might try ZoneAlarm or Windows 10 Firewall Control, which works just fine on Windows 11 too but weirdly retains its old name. (There are other options on both platforms, too.) I can't say that you'll like using them, and most people don't need them, but they can in some cases be useful in protecting your privacy.

Beware Analog Snooping, Too

I frequent coffee shops that are full of people with laptops, sometimes seated quite close to other customers. I'd have little difficulty positioning myself such that I could watch someone type a password. An incautious person could also have private information stolen while entering a PIN at an ATM or retail counter, scanning a passport at the airport, using a smartphone on the bus, or even talking loudly on a mobile phone.

When it comes to online privacy, this sort of low-tech snooping is just as much of a threat as hackers hunched over their keyboards in dark rooms far away. Be prudent when using your electronics in public—always keep an eye out for people keeping an eye on you!

High-Risk Resources: Internet Connection

If you know or suspect that you are at a high risk for being targeted individually, treat everything in this chapter as a requirement rather than a suggestion. Namely:

- Always use WPA for Wi-Fi connections; better yet, use wired Ethernet when possible.
- Use a (good) VPN all the time.
- Switch to an enhanced DNS provider (keeping in mind that VPNs typically use their own DNS servers).
- Install and use a good anti-malware app.
- Turn off any non-essential sharing features.
- If possible, disable your devices' cameras and microphones, or at the very least, physically cover your cameras.
- Use both inbound and outbound firewalls.

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,

you could always, you know, *not do that*. Regardless of what you do to protect your privacy, someone will probably find out and it will end badly for you. So seriously, *stop it*.

For what I'll call "lesser offenses," you'll want to be aware of, and take steps to avoid, certain types of data collection.

On Your Device

On your computer or mobile device, you should be aware that browsing the web typically results in *at least* the following information being stored, for each browser you use:

- **Browsing history:** A list of every webpage you've visited, in each browser.
- **Download history:** A list of every file you've downloaded—again, in each browser.
- **Cookies:** Information stored on your device by the sites you visit, or by the companies who place ads or other code on those sites. Cookies (see Live Data, ahead) are most often simple settings or random-looking strings of characters that identify your browser session uniquely, but they could also include your username, password, location, and any number of other details. Cookies can then be read when you revisit the same site—or *other* sites using the same ad network, analytics service, or social networking software.
- **Zombie cookies:** Conventional HTTP cookies aren't the only way browsers can store persistent data about your behavior. Records similar to cookies can be stored separately when you visit sites with content that uses HTML5 web storage and numerous other mechanisms. In some cases, the effect is to resurrect conventional cookies even after you've deleted them; hence the nickname zombie cookies.
- **Web caches:** The contents of pages you've visited recently, especially images (so the page can load more quickly if you return to it) and *favicons* (the little icons that appear in your browser's address bar next to the URL). Some browsers also store thumbnail images of the pages you've visited.

The above is only a partial list. Some sites use even sneakier techniques to squirrel away various information about you in a variety of places (see Live Data, ahead, for further detail). In addition to all these things, your device may store a global cache of recent DNS lookups—that is, somewhere outside your browser there may be a list of the domain names you (or your apps) most recently visited along with their IP addresses. If you're sufficiently curious or motivated to want to remove this cache, you can search the web for "delete DNS cache" to find the procedure for your operating system.

In Transit

The worry about web transactions being observed in transit is that data such as passwords, credit card numbers, photos, messages, and other personally identifiable information could fall into the wrong hands. In fact, the sky's the limit—anything you type on a webpage or any content displayed on a webpage you view—could get out. Fortunately, this is the least likely privacy threat when it comes to browsing the web and the easiest one to guard against (see the sidebar What About HTTPS?, ahead, and also refer back to Keep Your Internet Connection Private).

On a Web Server

Modern web servers can store an astonishing number of facts about every single page request, including (but not limited to) the following:

- **Time stamp:** The date and time of the request.
- **Time zone:** The reported time zone of the requesting device.
- **IP address:** The numeric address of the device you're using, which may or may not uniquely point to you, but which normally does reveal your approximate geographical location.
- **Item requested:** The URL and size of the page or other resource you loaded. If you visit a page that contains 20 graphics, they'll register as 20 separate requests.
- **Referrer:** The URL of the page on which you clicked a link to get to this page (if applicable).

- **Search terms:** If you reached this page from a search engine, the terms you searched for may be logged.
- **User agent:** The name and version of your browser. (Many browsers let you change this at will, so what the site records may only be what you *tell* it your browser is.)
- **Operating system:** Your operating system's name and version.

Note: For a variety of reasons, your reported browser and operating system names may not be accurate.

- **System fonts:** All the fonts installed on your device.
- **Screen characteristics:** The dimensions (in pixels) of your screen, along with color depth.

Furthermore, the server may be able to tell how far down a page you scrolled, how long you spent looking at a page, any items your pointer may have hovered over, which links to external sites you clicked, and a good deal more.

Although none of these items has your name on it as such (again, assuming you haven't logged in with unique credentials), you can probably see how a combination of them might point to you uniquely. And if that isn't already obvious, I invite you to visit a site run by the Electronic Frontier Foundation (EFF) called Cover Your Tracks. It examines much of the above data to create a "fingerprint" of the device you're using, and it tells you how unique that fingerprint is. I tested Safari on one of my Macs and found that it had a completely unique fingerprint among all those the site had tested recently. That means an advertiser (or anyone else monitoring my web activities) could be reasonably certain that I was the person who requested any given webpage, even without cookies or other tracking methods.

Choose a Better Browser

In the remainder of this chapter, I'm going to talk about ways of using your web browser (settings, practices, plugins, extensions and so on) that will improve your privacy. These all assume, however, that you're using a browser that doesn't respect your privacy as well as it should in the first place. If you're committed to using some particular browser, and that browser forces you to go out of your way to maintain some semblance of privacy, well, I guess you do what you gotta do.

But I think it's worth noting here that there are lots of browsers out there, and some of them are especially good when it comes to privacy. Use a great browser, and a lot of these problems go away by themselves (or, at least, with less effort than you'd otherwise need). Most browsers are free, so you have little to lose and lots to gain by doing most or all of your browsing in a better browser. (And remember, you don't have to use *just one* browser, either; you can use different browsers for different tasks, if you like.)

Browsers You Should Avoid

Which browsers should you stay away from? I can't give you an exhaustive list, but let me call out the top offenders:

Google Chrome

I hate to break it to you, but while Chrome may be the world's most popular browser, it's *terrible* when it comes to privacy. Although you can take certain steps to make it less awful (see If You Have to Use Chrome), there's a better path, which is to use one of the alternative browsers that are based on the same underlying Chromium engine, support all the same extensions, and work just as well on all your favorite websites. That is to say: you can have the Chrome experience, if that's what you want, without using Chrome as such. I wanted to be clear about this from the get-go, because I know how much people love Chrome—and also how dangerous it is. (We'll come back to the alternatives in a moment; see Browsers You Should Consider.)

I could write an entire chapter about Chrome's privacy sins, but let me summarize. Chrome is made by Google, and the browser's purpose is to make Google money. As you know, Google's income is mainly from advertising! So, Chrome is designed to capture and funnel as much information about you as possible to Google so that they can target ads at you ever more effectively. Chrome uses every technique in the book, including some rather sneaky and underhanded ones, to keep that information flowing—without your knowledge and, in some cases, even when you think you're following the most privacy-conscious practices. For example:

Invisible profiling (and more):
A 30-page web comic called Contra Chrome by Leah Elliott meticulously documents how Chrome creates an online profile that vacuums up every detail of what you do in the app, such as your searches (including partial words and phrases you entered before even pressing Return), the sites you visit, the links you click, the videos you watch, and where you're physically located. (Yes, even if you use Incognito Mode; see Private Browsing Modes.) It describes how Chrome may continue gathering information about you even when you tell it not to. And it describes the nefarious ways in which that data can be used. It also talks about how Chrome's moves to block third-party tracking cookies (which Google has since backtracked on) actually come with a different, sneakier technique that helps Google to track you better. It's…bleak. Many of these issues are echoed in It's time to ditch Chrome by Kate O'Flaherty in Wired.

Forced login by default:
This was mentioned in the web comic above, but it deserves special mention. Let's say you open Chrome and then visit some Google site, such as Gmail, Google Docs, or YouTube. When you log in on that one specific site, by default, Chrome *also* logs the browser itself in to your Google account, without asking for permission or confirmation. That, in turn, means that anything you do on *any* site in Chrome is potentially visible to Google. (Mind you: it doesn't guarantee that Google will spy on everything you do, but it opens a conduit that could be used for

that purpose.) What's worse, Chrome does this auto-login in such a way that it's barely perceptible.

When this feature first appeared in 2018, it caused an uproar (see, for example, Why I'm done with Chrome by Matthew Green, a cryptographer and professor at Johns Hopkins University). Eventually Google created a way to opt out of this behavior (see If You Have to Use Chrome), but it's far from obvious.

Misleading Incognito Mode:
As I discuss ahead in Private Browsing Modes, Chrome's Incognito Mode was designed only to prevent *local* storage of browsing data, not to keep it out of Google's hands. But the feature was designed in such a way that users thought their data was safe from Google in Incognito Mode, and after a huge legal hullabaloo, Google made changes to Chrome to clarify things. Nonetheless, Google is still collecting your browsing data in Incognito Mode!

Chrome has still other strikes against it, but I'll leave it at that. Long story short: if you have the option, avoid Chrome.

Brave

In earlier editions of this book, I recommended Brave, a browser based on the same Chromium engine that powers Chrome, that was ostensibly designed for much greater privacy while retaining all of Chrome's core features. It even offers an integrated option to use Tor—see Browse Anonymously—and automatically blocks most ads and trackers. All that sounds just fine on paper, and in fact if you're looking solely at Brave's privacy cred, it's pretty good. Even so, I'm no longer recommending Brave, for two primary reasons:

- **The company has done some shady things.** Brave was designed by and for people who are on the cryptocurrency bandwagon. That puts me on yellow alert, but isn't, by itself, a problem in terms of privacy. However, in 2020 there was a major scandal in which Brave was caught inserting its own affiliate links into URLs for cryptocurrency sites users searched for in Brave. In other words, they were surreptitiously making money off of users' searches. (See,

for example, Brave browser CEO apologizes for automatically adding affiliate links to cryptocurrency URLs by Kim Lyons at The Verge.) More recently, in 2023, Brave was accused of scraping copyrighted data and selling it for training AI models (see Brave Browser Under Fire For Alleged Sale Of Copyrighted Data by Matt G. Southern at Search Engine Journal). Those are just a couple of examples of behavior that strikes me as suspect.

- **I have some issues with the founder.** Brendan Eich, a co-founder of Mozilla and the creator of both Firefox and JavaScript, founded and still runs Brave. He was forced to resign from Mozilla because of a scandal involving his opposition to gay rights, and later got in trouble again for public comments disparaging masking and other public health measures during the COVID-19 pandemic. As many people have pointed out, his personal opinions have nothing whatsoever to do with the browser his company makes. But, again, they give me a bad feeling that makes me want to go in another direction.

If Brave were the only reasonable option in town, I'd use it despite my misgivings. But there are many other fine options (see Browsers You Should Consider, ahead) that don't push any of my ethical buttons.

Microsoft Edge

Edge, like Brave, is based on Chromium. It's Microsoft's default browser on Windows, but also available for other platforms (including macOS). It's way better than Internet Explorer; I'll give it that. However, Edge's privacy profile is very bad.

For example, by default, Edge sends *everything you type* in the browser, which could include passwords, to Microsoft for "writing assistance." So many of Edge's default settings send information of various kinds to Microsoft that unless you carefully study and adjust all your settings, nothing you do in the browser should be considered private.

As I write this in mid-2024, Edge is also the only Chromium-based browser I'm aware of that plans to adopt Goggle's so-called Privacy Sandbox, the feature I alluded to earlier that blocks third-party track-

ing cookies while scooping up more data for Google to use in serving you ads. Microsoft (and Google) will benefit more from your use of Edge than you will.

Browsers You Should Consider

If not Chrome, Brave, or Edge, then…what?

Don't worry. You have many excellent options. Here are my top picks:

- **Safari:** If you're an Apple user, you've at least encountered Safari, and it may already be the default browser on some or all of your devices. I find both its performance and its feature set to be excellent. It has numerous built-in privacy features that make it a reasonably good choice even with default settings (refer back to Discover Apple-Specific Privacy Features, earlier), though I would certainly make a few changes, such as switching the default search engine (see Search Privately) and adding an ad blocker (see Block Ads). Safari also integrates directly with the system keychain and Apple's Passwords app (for saving passwords) and privacy-specific features of Apple's iCloud and iCloud+ services, if you use those.
- **Firefox:** Firefox has a solid set of privacy features, though as with Safari, I'd tweak a few things from their defaults. Unlike Chrome and Chromium-based browsers, Firefox uses its very own rendering engine and extensions, so it doesn't feed into the Google ecosystem unless you want it to. It's a little quirky! And it doesn't have all the flashy features of Safari. But it's a solid, reliable browser. A separate mobile version of Firefox with even more privacy features, Firefox Focus, is available only for iOS/iPadOS and Android.

Note: There's also Tor Browser (see Browse Anonymously), a customized version of Firefox that offers even more privacy, at the cost of speed and compatibility.

- **Orion:** The Orion browser, created by the developers of the privacy-focused search engine Kagi, is based on Apple's WebKit framework and looks *almost* like a Safari clone (with added privacy features, such as built-in ad blocking). But unlike Safari, Orion

supports both Chrome and Firefox extensions, making it considerably more versatile. I've been using it as my primary browser for several months, after having been a dyed-in-the-wool Safari fan for many years. Currently, Orion is available only for Mac, iPhone, and iPad.

If, however, you prefer a Chromium-based browser that looks and acts more like Chrome—and can use all the same extensions—I have some additional recommendations:

- **Vivaldi:** When I need a Chrome-compatible browser (because sadly, even in 2025, some sites simply don't work in Firefox, Safari, or other WebKit-based browsers like Orion), I turn to Vivaldi. It's a privacy-focused browser that can block most ads and tracking. I've never encountered a site that works in Chrome but not in Vivaldi.
- **Comodo Dragon and IceDragon:** Comodo is a company best known as an issuer of SSL security certificates and other security products. They offer two browsers—for Windows only, sorry—that make me smile just because of their names. Comodo Dragon (get it?) is based on Chromium, while Comodo IceDragon is based on Firefox (and, I guess, designed to appeal to *Game of Thrones* fans). They both have a full range of privacy and security features built in.
- **Epic:** Epic Privacy Browser has an optional built-in encrypted proxy (much like a VPN), and blocks most ads and trackers as well as making it more difficult for sites to identify you using browser fingerprinting.

Even if you are running one of the above browsers, I strongly recommend reading the rest of this chapter and double-checking all relevant settings. Never assume your app will do all the right things automatically.

If You Have to Use Chrome

Perhaps you're using a computer or mobile device that's managed by your employer or school, and it's either impossible or against the rules to install any browser but Chrome. What can you do to reduce the privacy risks? Follow these steps:

1. If you're currently signed in to your Google account, click your avatar in the top-right corner of the window and click "Sign out."
2. Go to Chrome's Settings page (enter `chrome://settings` in the omnibox).
3. Click "You and Google" on the left. Then, under your profile name (which may be something generic, like "Person 1"), click "Sync and Google services" and turn off everything, but *especially* the top item ("Allow Chrome sign-in"), which automatically logs you in to your Google account when you log in to any Google-affiliated site.
4. Click "Privacy and security" on the left. Then:
    - Under "Third-party cookies,"make sure "Block third-party cookies" is selected.
    - Under "Ad privacy," turn off "Ad topics," "Site-suggested ads," and "Ad measurement."
    - Under "Security," select "Standard protection" and turn off "Help improve security on the web for everyone." Also turn on "Use secure DNS" and choose either NextDNS, Cloudflare (1.1.1.1), or OpenDNS from the pop-up menu.
5. Quit and reopen Chrome. *Do not skip this step!* Until you relaunch Chrome, the change you made in step 3 won't take effect.

Later in this chapter, I discuss other steps you can potentially take, such as installing ad blockers, but these settings will address the most egregious issues. Do keep in mind, however, that Google is constantly making changes to Chrome, and by the time you read this, the settings could have changed. Be on the lookout for new—or slightly reworked—settings that turn themselves on by default!

Note: Most Chromium-based browsers have similar settings, though their names and locations might be somewhat different.

Go to the Right Site

One of the most surprising privacy threats on the web is impostor sites that look almost exactly like the real thing, but are merely clever copies designed to trick you into supplying your password, credit card number, or other private data. Sometimes these sites appear if you make a slight typing error when entering a URL or if your DNS settings have been compromised, but they're most commonly reached by clicking a link in a phishing email or text message. (These messages often warn you that you must "update" or "confirm" your account settings or suffer dire consequences.) Phishing via other avenues, such as X, Facebook, Instagram, iMessage, WhatsApp, SMS, Discord, Twitch, YouTube, TikTok, and even sneakily added calendar entries, has also become more common.

Note: Apple's Messages app (which can use both the iMessage protocol and SMS) "helpfully" displays thumbnails of any webpages linked from incoming messages. You can't turn this feature off unless you engage Lockdown Mode, and it's a pity, because it means merely receiving a message can cause a webpage to load (revealing information about you in the process). You can, however, alter links in *outgoing* messages to avoid having preview thumbnails appear.

Here are some tips to avoid bogus sites:

- If you haven't already done so, follow the advice in Avoid DNS Mischief, in the previous chapter, to avoid most DNS exploits.
- Don't click links in email messages (or in SMS or other sorts of text messages), if you're not absolutely sure of the sender. If a message that appears to be from your bank, PayPal, Amazon, Apple, or whoever insists that you log in to correct some problem and you're worried that it might be a legitimate message, open your web browser and *manually* type the site's address, making sure you're using HTTPS. Then log in and see if there are any messages waiting for you. If not, the message is almost certainly fake.

- On Mac and Windows systems, hovering over a link in an email message or webpage usually reveals the link's URL before you click it. If it looks in any way suspicious (see above), don't click it: instead, try navigating to the site manually. On mobile devices, many apps will try to show you the destination URL inline, since there is no way to hover. In Safari for iOS, tapping and holding a link reveals the URL and some options.
- Avoid clicking links from URL-shortening services like bit.ly, goo.gl, and TinyURL without first checking their destination using a tool like unshorten.it or unshorten.me. Although there are legitimate uses for URL-shortening services (indeed, I frequently use them myself in Take Control books), they're often abused to obscure bogus and dangerous links.
- Check the site's certificate. Real banking, commerce, and similar sites invariably use HTTPS (see the sidebar just ahead), and you can usually click a lock icon in your browser's address bar to verify the site's SSL certificate. If there's no certificate, if you see a certificate warning, or if the site doesn't even use HTTPS, you may be dealing with an impostor.
- Let technology help. Most browsers have built-in checks to warn you of sites that might be bogus (see Browser Privacy Settings), as do some third-party plugins (see Block Ads). Be sure to enable these features. In addition, most password managers (see Protect Passwords and Credit Card Info) confirm each site's identity before entering your credentials.

What About HTTPS?

When the first edition of this book was published in 2013, a large percentage of the world's websites used plain, unencrypted HTTP instead of HTTPS, which encrypts data that travels between your browser and the site. Such sites carry a certain amount of risk that someone could eavesdrop on the data you send and receive, so I had to explain the importance of looking for the little lock icon in your browser's address bar and being cautious of sites that didn't offer encryption.

The world has changed since then. Thanks in large part to free tools for web developers such as Let's Encrypt, HTTPS websites are now the norm, and major browsers often switch automatically to HTTPS if a site supports it (even if you enter a plain `http://` URL). For all practical purposes, you don't have to worry about that anymore.

Say No to Selling Your Personal Info

You'll often see links on websites (sometimes at the bottom of a home-page; sometimes in a banner or pop-up alert) that say "Do not sell my personal information" (or words to that effect). These links exist mainly to comply with California's Consumer Privacy Act (or similar laws elsewhere). These links let you opt out of any sale of your personal information collected by that site. Unfortunately, the California Consumer Privacy Act doesn't apply to all websites or businesses; there are many qualifications and exceptions. Even so, every little bit helps. If you ever see a link like this, *immediately click it and follow the steps to opt out*.

It astonishes me that anyone, having been informed that their personal information is being sold to data brokers and advertisers, would shrug and let it happen. Yet many people do exactly that. Don't be one of them! Given the choice, always opt out. Letting a site sell your information lets them make money at your expense, without benefitting you in any way.

Manage Local Storage of Private Data

In On Your Device, I mentioned several types of (potentially) private data that may be stored on your device as you browse or use internet-enabled applications. Here, I want to provide a bit more detail about this data and tell you what you can do about it.

It may be helpful to conceptually divide the stored data into two categories: *live data*—that is, information that may be sent from your browser to the sites you visit in real time—and *historical data*, which is accumulated on your device but not transmitted. Both types of data are normally stored separately for each browser you use, on each device.

Live Data

When you visit a site and it sets a cookie, that by itself is generally harmless; it's just a bit of text stored on your device. When you visit the same site later, it will read that cookie before displaying the page. Cookies are often helpful because they enable sites to save preferences for you, keep track of your login information so you need not enter your credentials each time you visit, and offer continuity (such as remembering which articles you have read) on successive visits.

Cookies have become a privacy problem because they're often used for tracking you *across sites*. When you load a webpage, it may include code for ads, social networking widgets, analytics services, or other resources that come from *other* sites. When those resources load, they can save cookies on your device that record information about you and what you did while viewing the site you're on. If the next site you visit happens to use an ad, widget, or code from the same network, it can read the cookie to see what you've done in the past, and add information about your current visit. This process continues indefinitely, such that you may randomly visit a site for the first time and instantly see ads that are mysteriously targeted to your interests and activities, including items you've searched for recently on Amazon, Google, or other sites.

In these cases, it's not the site you're visiting that's setting and reading tracking cookies, but another site or network that has placed code on the page to track you. That's why you'll see these types of cookies referred to as *third-party cookies*. A site may use its own cookies (first-party cookies) for useful purposes such as saving your preferences but permit third parties to use cookies for tracking and other less-noble reasons. Some popular news sites have *hundreds* of tracking cookies, which pose a privacy risk and cause pages to load much more slowly (and help chew through your data cap). (Browsers don't normally go out of their way to tell you what cookies a given page has set, but see Block Ads, ahead, to learn one way to avoid them.)

Browser cookies aren't the only sort of live data that your device may store and send to sites as you browse. For example, some especially aggressive trackers use a variety of techniques (sometimes known as evercookies or zombie cookies) to *respawn* cookies you've deleted or to track you using other methods involving your image cache, JavaScript, and/or HTML5 web storage.

What's HTML5 web storage, you ask? It's another way a webpage or application can store data within your browser and access it later. It was designed to be not only faster and more secure than cookies, but also to hold larger quantities of data. And in principle there's nothing wrong with it—HTML5 web storage can do neat things like cache web-mail or map images so that you can read them offline. But it's still an imperfect system that can be used for undesirable purposes.

Historical Data

Cookies normally stick around on your device for quite some time, so in addition to sending live data about you as you browse the web, they serve as historical evidence of the sites you've visited and some of the activities you've performed there.

Your browser may also store lists of pages you've visited (browsing history), files you've downloaded (download history), searches you've performed (search history), and information you've entered into form fields. Barring a bug or malicious exploit, your browser doesn't trans-

mit any of this data, but someone could examine your device after the fact and get a detailed record of where you've been.

Note: Did I say "malicious exploit"? Such things do happen—including utilities that secretly send your browser history to the developers. That's very much against the rules, especially in Apple's App Stores, but companies still manage to cheat from time to time.

As I said earlier, live data and historical data have entirely different privacy implications. You may find live tracking to be creepy and offensive but have no qualms about someone examining the browsing history on your computer; or you may have no issues with advertisers knowing what you're up to but prefer to keep that information from, say, your employer (who might take a look at your computer when you're not at your desk—or even use monitoring software).

Avoid or Remove Local Data

Broadly speaking, you can manage local data storage in either of two ways:

- Prevent data from being stored on your device in the first place—using browser settings, a private browsing mode, or third-party plugins/extensions.
- Erase stored data after the fact.

I think most people would agree it's preferable to avoid getting sick than to cure an illness. By preventing data from being stored locally in the first place, you eliminate both the threat of live tracking and the potential for historical examination. Furthermore, clearing cookies and other local data after the fact may prevent you from being tracked from one session to the next, but not during a single session.

However, depending on your browser, operating system, and device, you may be unable to prevent data from being stored—or at least not with the granularity you prefer. For example, if a browser's only option is to block *all* cookies, that may make your web browsing experience worse because it prevents the use of any helpful, first-party cookies.

So, what are your options for managing local data?

Private Browsing Modes

Safari, Firefox, and Vivaldi have Private Browsing (in Safari, choose Safari > Private Browsing; in Firefox or Vivaldi, choose File > New Private Window). Google Chrome has Incognito windows (choose File > New Incognito Window; see **Figure 14**). Edge has InPrivate (click More `···` > New InPrivate Window). Virtually all other browsers have something similar.

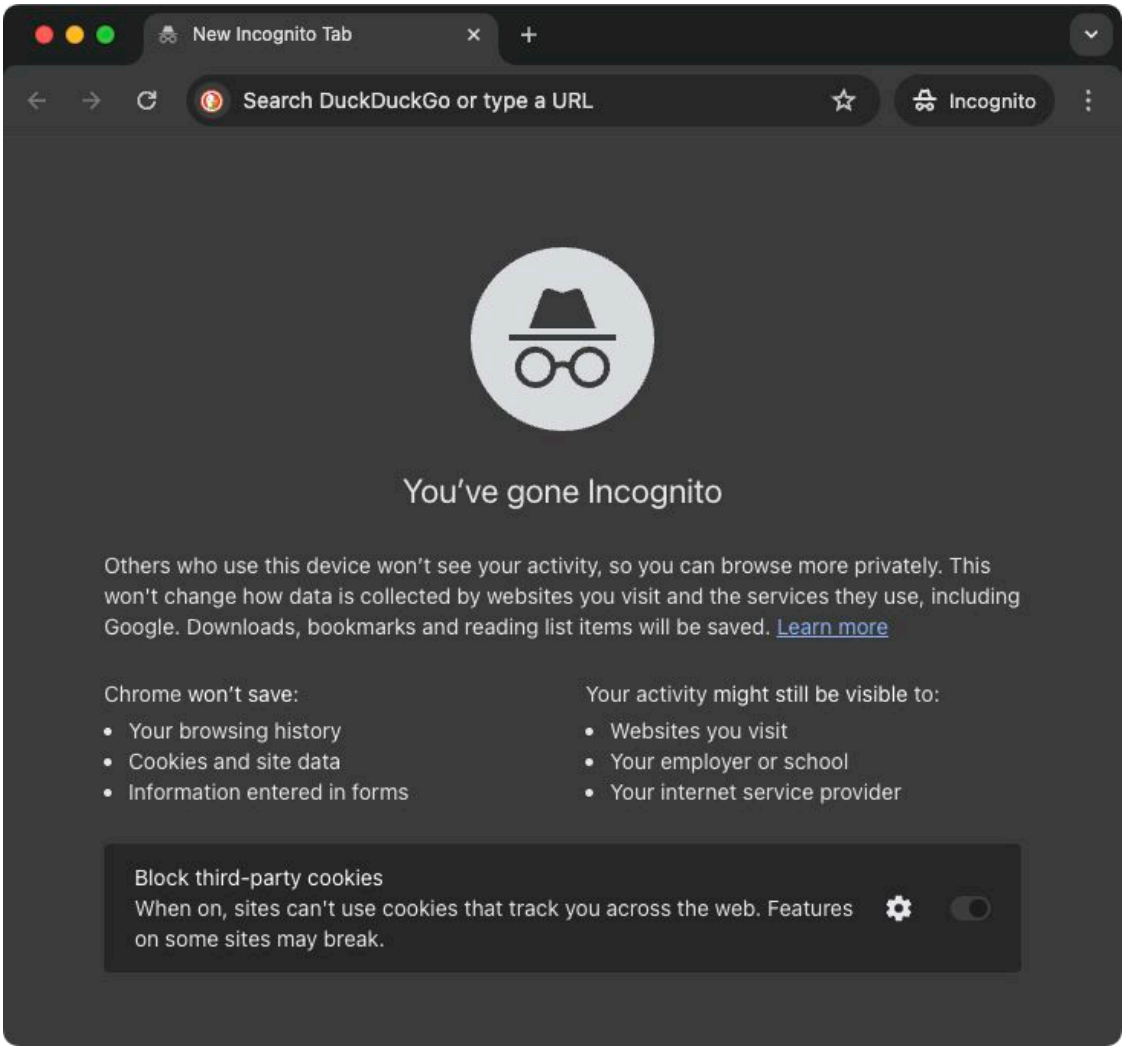


Figure 14: Chrome's Incognito window spells out what information it protects, as well as what possible privacy risks remain.

While you're in one of these modes, your browser typically avoids storing data such as cookies; browsing, download, and search histories; form/autofill data; and page or image caches. Because the data isn't

stored on your device at all, private browsing thwarts tracking based on reading on-device files as well as after-the-fact analysis.

However, that's all private browsing does. Which is to say: it doesn't actually keep your browsing private! It's certainly not private from the websites you visit or from your ISP, for example. Although it does reduce some forms of tracking, its main point has always been to prevent someone else from finding out what you did on the web by examining your device after the fact. To be sure, there's sometimes utility in that, but it's far from complete privacy.

I've always known this was the case, but apparently a lot of people do not. That's why Google was the subject of a class-action lawsuit brought by users complaining that the company continued to gather and store information about their searches and browsing history even when Chrome's Incognito Mode was enabled. (I mean, *of course* Google did that. It's Google, remember, and besides, they always said that Incognito Mode was solely about what's saved *on your device*.) As a result, Google agreed to delete their records of data that had been collected when Incognito Mode was in use, and modify Chrome's "You've gone incognito" message to make it clearer what happens.

Despite the limitations, I recommend private web browsing modes for people who want extra privacy for specific sites or tasks. Use a private browser window when you need one; use a normal window when you don't. That way, the bulk of your browsing has the benefits of first-party cookies, histories, and so forth, but private things stay private.

However, please keep the following in mind about private browsing:

- The sites you visit with private browsing still collect all the usual information about your device and actions, just as they would any other visitor. (See On a Web Server, above.) To websites, "private browsing" is the same as non-private browsing.
- Plugins and extensions could still store data locally if they remain enabled, and there's no guarantee that an unscrupulous tracker hasn't invented some other sneaky trick to store data even when browsing privately. *Browser beware.*

- If you download a file, that file may not appear in your download history, but it'll still be on your device (or perhaps even in your cloud-based storage).
- Private browsing won't stop you from *manually* bookmarking pages.
- Although your browser doesn't store search terms while browsing privately, the search engine might (see Search Privately).
- DNS queries, which happen outside your browser, could still be cached on your device.
- Someone sniffing your internet connection may still be able to see what sites you connect to, and server logs will still be kept.

Browser Privacy Settings

Whereas private browsing modes are temporary, you can usually fine-tune a browser's preferences to specify permanent settings for which sorts of data should be stored locally (**Figure 15**). You can usually also examine or delete data already stored.

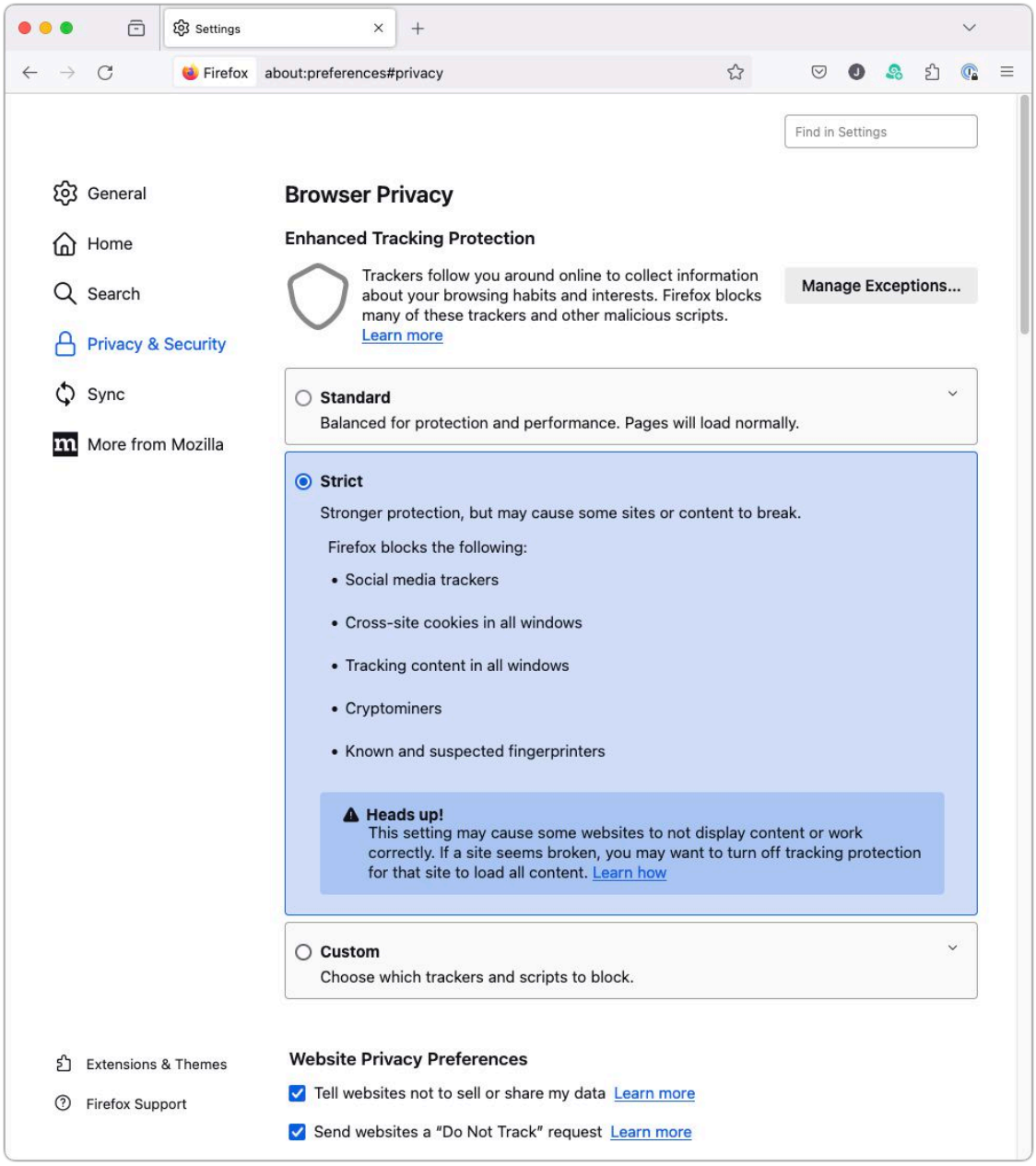


Figure 15: Firefox offers a variety of privacy settings; most other browsers have a similar range of options.

Once again, the range of choices varies by browser and platform, and I can't cover every detail here. I will say, however, that you can usually make at least the following choices:

- **Cookies:** Block all cookies; accept all cookies; or (my recommendation) block only third-party cookies. You can also usually view all the stored cookies and delete any of them by site, or all of them en masse. (As I mentioned earlier in Intelligent Tracking Protection, Safari has a different spin on this, a feature that temporarily stores, then deletes, third-party tracking cookies.)

- **Do Not Track:** Your browser may be able to ask sites not to track you, and I suggest you enable this feature—but most sites ignore the request, and merely enabling the feature could in some cases make you more identifiable. (See the sidebar Do Not Track, ahead.)
- **Phishing and malware protection:** Alert you to sites that may be fraudulent (especially phishing sites) and those suspected of containing malware. By all means, turn this on.
- **Location tracking:** Your browser may report your location in order to provide more useful results (for example, local weather, movie times, and stores) without your having to manually specify where you are. I usually find location tracking helpful, and I figure I'm already giving away my general location by my IP address when not using Tor (see Browse Anonymously, ahead) or a VPN, so this isn't much worse—although, to be fair, location data derived from Wi-Fi triangulation and GPS can be much more precise than what your IP address alone indicates. You can usually enable or disable location tracking on a per-site basis or globally, as you prefer.
- **Search suggestions and history:** When you start typing a search term, your browser may try to fill in the rest for you as a convenience feature. To do so, it may use a locally stored list of your previous searches, but it's probably also telling the search engine what you've typed so far (each and every keystroke!) and asking for a list of matches. This can sometimes reveal more about you than your search terms alone. You can turn these features off.

Note: Chrome and Edge send literally everything you type in your browser to Google or Microsoft, by default, for the purpose of spell checking! But that could even include passwords. To turn this off in Chrome, go to Chrome > Settings > Languages and either select "Basic spell check" or turn off "Check for spelling errors when you type text on web pages." In Edge, go to Edge > Settings > Languages, and in the "Writing assistance" section, turn everything off.

Here's how to access privacy settings in selected desktop browsers:

- **Edge:** Click More `···` > Settings, click "View advanced settings," and scroll down to "Privacy and services."
- **Firefox:** Enter `about:preferences` into the address bar, then click Privacy & Security in the sidebar.
- **Google Chrome:** Enter `chrome:settings` in the address bar. Then click "Privacy and security" in the sidebar and work your way through each of the categories.
- **Safari:** Choose Safari > Settings and click Privacy. Also click Websites for some additional privacy-related settings.
- **Vivaldi:** Enter `vivaldi:settings` in the address bar. Then click Privacy and Security in the sidebar.

Do Not Track

Most modern browsers can (at your option) transmit a special Do Not Track header when they load a webpage that asks the site to pretty please not track your visit. And you should turn this feature on because some sites will heed your request, and even those that don't should know that you prefer it that way.

Unfortunately, Do Not Track is merely a request. Advertisers, data brokers, and analytics firms are free to ignore it, and most do—the standard is all but dead. For this reason, Apple dropped Do Not Track support in Safari 12.1 and later in favor of its Intelligent Tracking Protection feature.

And, ironically, now that Do Not Track is used less frequently, the mere fact that you have it turned off could make your browser fingerprint slightly more unique, and thus make your behavior a bit easier to track!

Block Ads

Besides using privacy-enhanced browsers like Vivaldi, private browsing modes, and better browser settings, you can also install extra

software to enhance your web privacy. I use the term "ad blockers" for this category of software, even though preventing ads from appearing may be just a small part of what they do.

As we all know, the web has become cluttered with ads everywhere, sometimes covering so much of a page that it's hard to find the actual content. Ads are a scourge for many reasons, and you may want to block them simply on the grounds that they're annoying or intrusive. However, for the purpose of this book, we're concerned primarily with how ads affect your privacy.

Since you've already read about the lengths advertisers (and companies supported by ad revenue) go to collect private information about you, it should come as little surprise that merely *loading* a webpage containing ads gives away data you probably want to keep private: it tells the company serving the ads your IP address (which probably reveals something about your location), the details of your browser and operating system (which can be used to identify you uniquely), the page you just came from, and more. In addition, merely by loading, ads can set and read cookies that can be used to track your activities across the web.

Even though there are other steps you can take to hide your IP address, disguise your fingerprint, and block cookies, the most effective way to deal with all those things at once is to prevent the ads from loading in the first place. Then you get a clutter-free screen as a lovely side effect.

Tip: For a truly upsetting and sobering look at all the places various websites are trying to send your data (even if you prevent that by blocking cookies, ads, and so forth), try the free Blacklight service from The Markup.

I couldn't begin to review the full range of options. So, I'll just give a few examples.

If you use Safari in macOS, iOS, or iPadOS, you'll need an Apple-sanctioned browser extension from the App Store—use this link (and note that it shows all kinds of Safari extensions, not just ad blockers). Of the ad blockers shown there, my current favorite (very much subject

to change) is AdGuard for Safari, which blocks most ads and trackers while allowing you to easily whitelist sites and customize which types of content are and are not blocked. Other highly rated extensions include 1Blocker and DuckDuckGo Privacy for Safari, though the choices change frequently.

For other Mac, Windows, and Android browsers, one tool I'm quite fond of is uBlock Origin. uBlock is highly customizable, letting you selectively or globally block ads, tracking cookies, social media buttons, and other potentially undesirable elements without interfering with normal browsing and local storage the way private browsing modes do. It also offers protection against domains known to host malware.

I previously recommended Adblock Plus, which has a comparable range of features. It works, but I have a philosophical problem with it: companies like Google and Amazon have paid to be on a list of exclusions so you'll still see their ads even if you use Adblock Plus. To opt out from seeing these ads, visit Adblock Plus's Options screen and deselect "Allow some non-intrusive advertising." Since avoiding ads and associated tracking is the whole point of Adblock Plus, you shouldn't give it any loopholes!

(The EFF also has a free blocker called Privacy Badger, which is based on the Adblock Plus code but without the creepy pay-to-play exclusions. However, it works only on Chrome/Chromium-based browsers, Edge, Firefox, and Opera.)

Note: Confusingly, there's also a browser extension called AdBlock (with a capital B and without the Plus), which does something similar without partnerships to permit "non-intrusive" ads.

Another fantastic free tool is called Ghostery—available as a cross-platform browser extension for most browsers (including Safari), not to mention a standalone iOS web browser. It displays a list of all trackers of various sorts—both honorable and ignoble—present on any given webpage (**Figure 16**) and lets you enable or disable them (individually or by category), which can be handy because some sites don't

work without certain trackers. It's highly educational as well as effective in increasing your privacy.



Figure 16: Ghostery optionally displays a list showing which advertisers and trackers it's blocking when you load a site; you can individually enable or disable them as you like.

Tip: Some privacy appliances also block ads—and can do so for all devices on your network, including ones like smart TVs that can't run their own ad-blocking software. See Consider a VPN Router or Privacy Appliance.

Unfortunately, even with the slickest ad blocker, you are guaranteed to see, from time to time, pop-up notices on websites urging you to disable your ad blocker—just for them!—because they depend on ad revenue to make money. Some of them ask nicely and give you a way to opt out; others (ad blocker blockers) refuse to load the page at all if they can't display their ads.

My response to such pop-ups, 100% of the time, is simple. If there's a link I can click or tap to opt out (like "Continue without supporting this time"), I use it. If not, I just close the page and do without whatever I was going to see there. I would not, under any circumstances, exempt a site from my ad blocker just so I could read an article or watch a video. I recommend that you take the same approach.

You'll read countless claims that websites *need* to show ads to stay in business and that your *shameful* refusal to let them is tantamount to *stealing* their content. But none of that is true. There are ways to make money that don't involve selling customers' personal information, and those very ads, the ones those sites want you to unblock, are the reason you installed an ad blocker in the first place! You have my permission to block ads everywhere and use the latest ad blocker technologies, without remorse.

Protect Passwords and Credit Card Info

Your passwords and credit card information are certainly among the items you'll most want to keep private, but you can't do very much on the internet without entering a password, and much online shopping requires entering a credit or debit card number. So you can't always avoid ever sending these things over the internet, but you can keep them private by using a password manager.

I've previously mentioned password managers—apps such as 1Password (**Figure 17**), Dashlane, and Bitwarden—that can generate, securely store, and enter passwords for you. Users of Apple devices can also use a built-in password manager called iCloud Keychain (see the sidebar Security in iMessage and Other Apple Services) and Wallet & Apple Pay for payment card management.

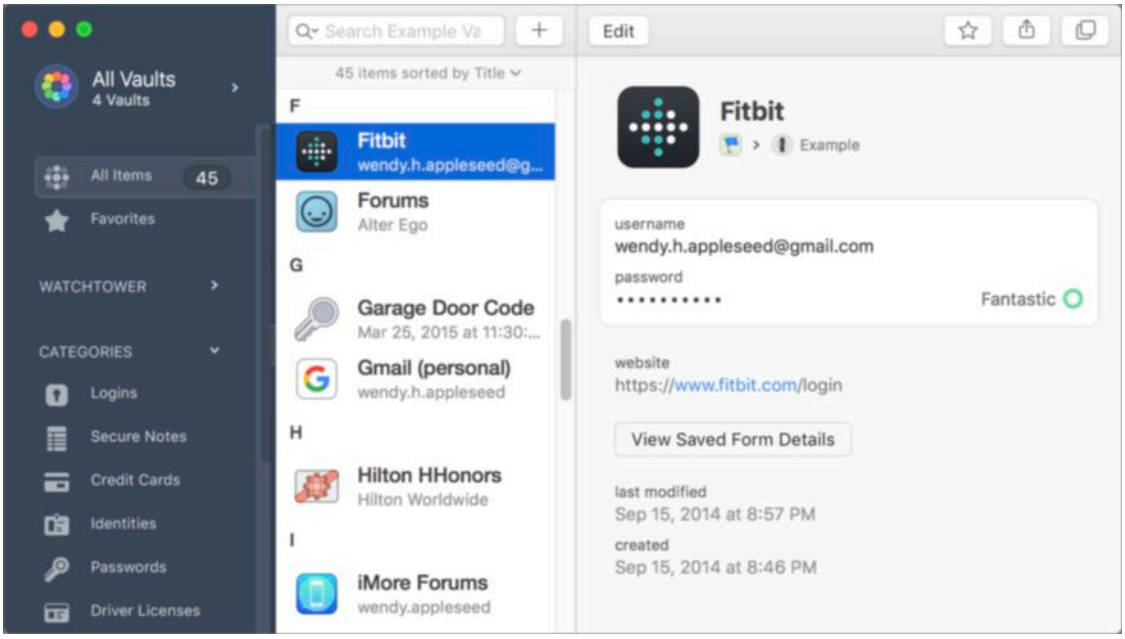


Figure 17: 1Password (Mac version shown here) securely stores passwords, credit card numbers, and other personal data, and syncs them among your devices.

Password managers can store not only passwords but also credit card numbers, secure notes, and other private data. In addition to their obvious benefits, these apps can verify that you're on the right website before handing over your password—yet another way to avoid phishing and DNS spoofing attacks.

Warning! Most browsers have built-in password-filling tools, but they tend to be both less capable and less secure than full-blown password managers, since they can sometimes be tricked into auto-filling information like email addresses and passwords without a user's knowledge.

I discuss password managers and other password strategies further in my book *Take Control of Your Passwords*. (And, if you decide to use 1Password as your password manager, you can read my book about that too: *Take Control of 1Password*.)

Note: Although password managers are generally quite secure, data breaches and exploits are possible. (LastPass, for example, suffered a series of security breaches so serious that I can no longer in good conscience recommend it as a safe way to store sensitive data.) Be sure to choose a strong master password, and respond promptly to any security alerts.

Later in this chapter, in Shop Online Privately, I discuss further issues involving online commerce.

Note: Sad to say, Google (and perhaps other companies) can even track your credit card usage *in many brick-and-mortar stores* and add that information to your personal advertising profile. Your best defense in situations like that is to use Apple Pay (discussed ahead) or cash. Sorry.

Search Privately

You know already that you can use a private browsing mode (or change your browser settings) to avoid having your search terms stored on your device. But the search engine could keep a record that someone at such-and-such an IP address performed a certain search at a certain time and date. Furthermore, if you're logged in to the search site—for example, you're logged in to your Google account while you do a Google search in the same browser—the site will store the search terms in your account, along with all the other data it collects about you. Later, you may use the same search engine on a different device and see those earlier terms pop up again! That could be either helpful or disconcerting.

Google lets you temporarily or permanently delete searches and other activity from your account (refer back to Remove Your Info from Google), and most other search providers do too. But they don't make it convenient, you might forget, or you might not do the right thing in every browser or on every device.

If you want to use a pretty good search engine that won't log your results, period, try DuckDuckGo, which is now available as a default search option in most modern browsers. All searches are completely anonymous. Nothing is logged, no tracking occurs…and you can disable ads in DuckDuckGo's settings. Although the results aren't always as thorough as with Google or Bing, DuckDuckGo is getting better all the time. Another search engine, called StartPage, which makes similar privacy claims and offers the option of using servers located only in Europe, if that's your preference—but because it's basically a proxy for Google, there's still a possibility of Google using browser fingerprinting and other techniques to identify you as an individual when you search. And you won't find StartPage integrated into as many browsers as DuckDuckGo.

If free search engines like those aren't cutting it for you, there's another option: you can *pay* for a really excellent search engine called Kagi that has no ads, tracking, or logging. It doesn't need them, because it makes money directly from its users! Kagi offers 100 searches for free; paid plans start at 300 searches each month for $5, or unlimited searches for $10 per month.

Keep in mind, however, that not all web searches happen in a browser! For example, system-wide searches in macOS and Windows 11 (including those initiated by voice, using Siri or Cortana) have internet components. Siri mostly relies on Google for web searches and Cortana, naturally, uses Bing by default, but both may also consult numerous other sources, including Wolfram Alpha. And any of these services may log your searches, along with your location and other data. Unfortunately, if you want the benefits of this type of text- or voice-based search, it comes with a certain loss of privacy by definition. However, you can in some cases limit the way searches occur; for example, on a Mac, you can go to System Settings > Spotlight (or Siri & Spotlight) and uncheck Conversion, Definition, Movies, Music, Other, Siri Suggestions, and Websites at the bottom of the window to restrict Spotlight to searching data on your Mac. On Windows, go to Settings > "Privacy & security" > "Search permissions" and turn off "Microsoft account" and "Work or School account."

Browse Anonymously

So far I've talked only about *private* web browsing, but sometimes you may need greater assurances that your web activities are *anonymous*, meaning they aren't associated with you individually.

Note: Never assume that anonymity on the internet is absolute or permanent. Anonymity means making it extremely difficult to discover your identity—and although that's often good enough, anonymous statements and activities can sometimes be traced back to the person who originated them.

I said in the Introduction that this is a book about ordinary privacy for ordinary people. And frankly, the picture I'm about to paint is far from ordinary. This is something a political dissident or a journalist in an authoritarian country might need to worry about, not a day-to-day privacy concern for regular folk. Still, it's worth knowing about.

Imagine that your local internet connection is encrypted using a VPN, which also hides your real IP address. Then you use your browser's private browsing mode to eliminate all local data storage, and connect to a web server using HTTPS, so the entire transaction is encrypted. That's about as private as you can get—it's extremely unlikely that any party between your device and the web server will be able to see your information, and similarly unlikely that anyone who examines your device later on will be able to discover evidence of the session either.

However, don't forget that the server still logs your visit. Server logs may provide enough other information (see On a Web Server to learn about browser fingerprints) to uniquely identify your computer. Furthermore, even though the server doesn't know your real IP address, your VPN provider does, and they may have kept a log of your session that could be traced back to you (perhaps through warrants or legal action). The VPN provider itself could also be run by an untrustworthy organization. Finally, even though an encrypted connection protects the contents of the transmitted data, it doesn't protect low-level routing information, which indicates the data's origin and destination. (Encryption can't hide this: intervening routers and switches

need that information to pass your data along.) So, by combining all that information, someone could still discover that you were the person who visited a certain page at a certain time. For certain types of web activity, that could put you in deep trouble.

If you need near-complete anonymity when browsing the web (including using webmail), you should know about Tor. Tor, which originally stood for "The Onion Router," is a system that not only encrypts data but also does so multiple times, sending it through a series of randomly selected relays called nodes (see **Figure 18**)—each of which knows only about the previous and next node in the chain, but not the information's origin (unless it happens to be the "entry" node) or destination (unless it's the "exit" node). This process makes it extremely difficult to determine the source of any web transaction.

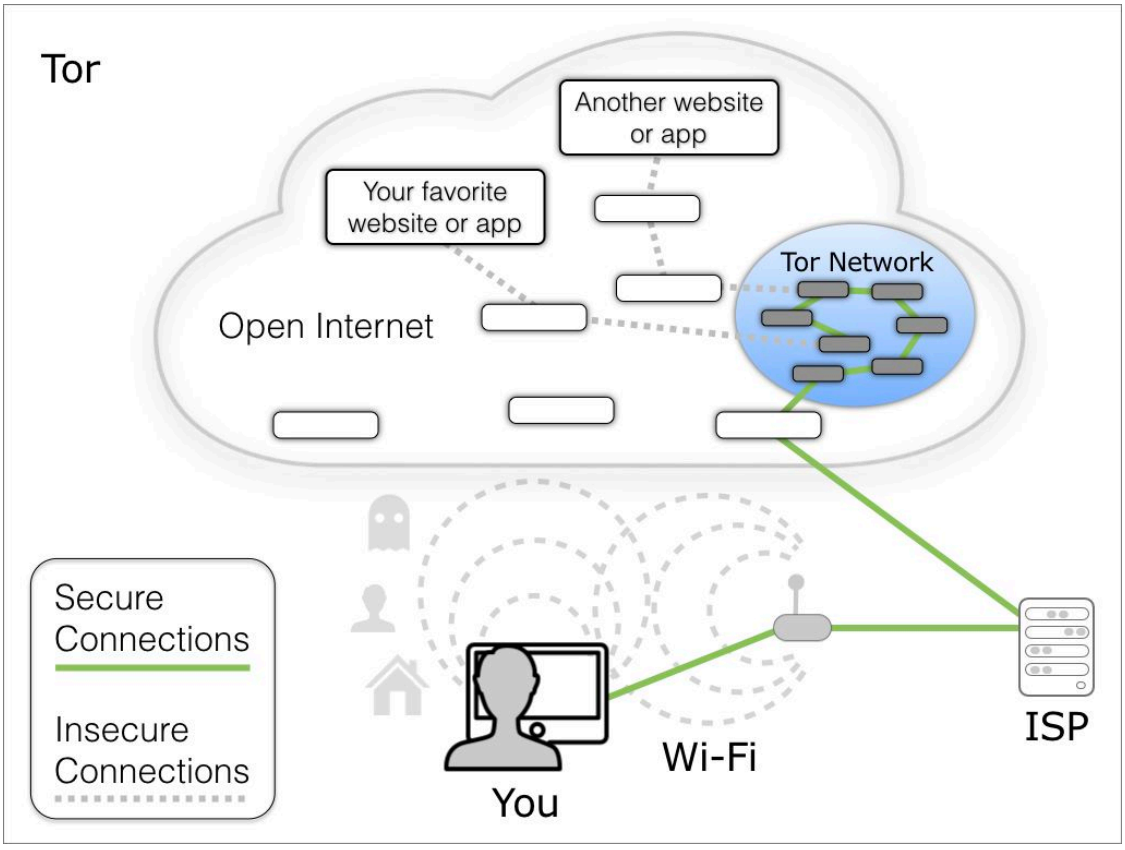


Figure 18: When you use Tor, your connection to any server goes through a random series of nodes, each one adding a layer of encryption and further obscuring the sources of requests.

To use Tor on a Mac or Windows PC, you download Tor Browser, which is a specially customized version of Firefox that includes strong

privacy settings plus the extra software needed to connect to the Tor network (**Figure 19**). Full instructions for installation and use are on the Tor site. For Android, you'll want Tor's Orbot package; for iOS and iPadOS, you can use the third-party Onion Browser.

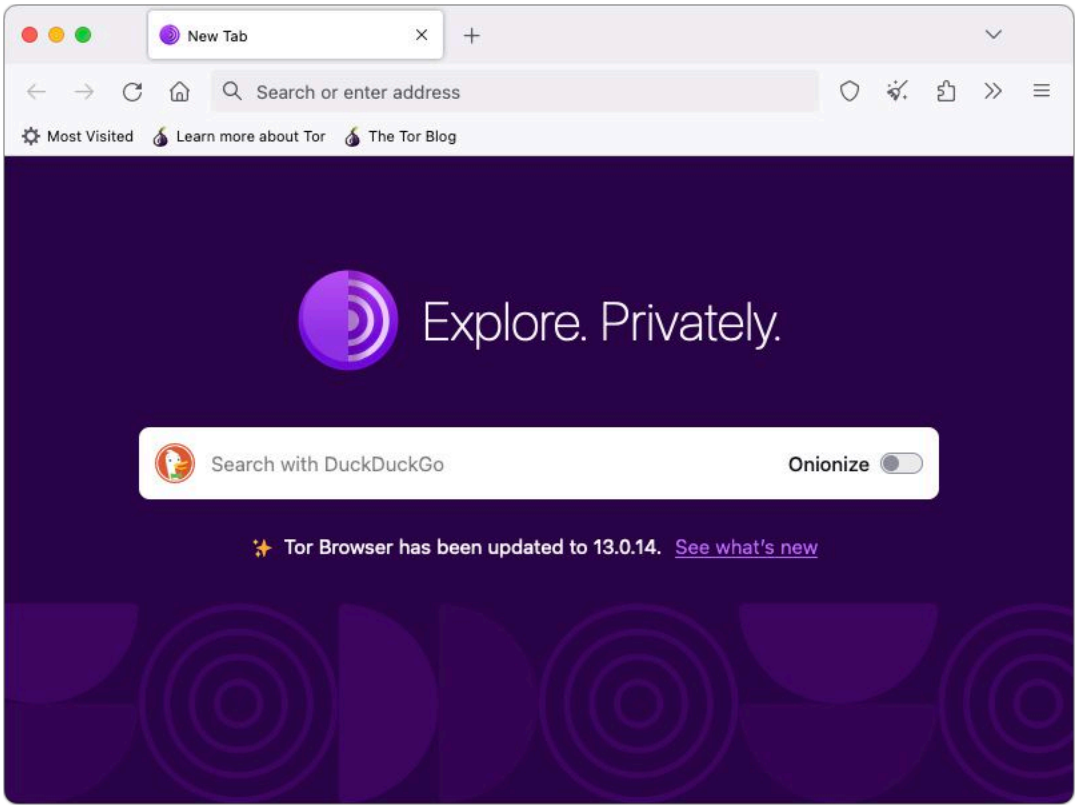


Figure 19: Tor Browser, a customized version of Firefox.

Tor can dramatically increase the chances that your web activities will be anonymous, but it's not without its drawbacks. For example:

- Several weaknesses in the Tor system have been discovered that could be exploited under the right conditions to reveal private data. For example, someone who runs a Tor exit node could monitor unencrypted traffic flowing between it and the rest of the internet—and indeed, it's widely believed that the FBI and other agencies run a large number of Tor exit nodes to do just that. Using end-to-end encryption such as TLS/SSL reduces the risk of eavesdropping significantly, even if the exit node is compromised.
- Someone monitoring your internet connection can tell that you're using Tor, even though they can't necessarily tell what you're doing with it. Some ISPs and countries block all known Tor traffic. There

are ways to work around this problem in some instances, but they make the process of web browsing that much more cumbersome.

- Merely using Tor could result in unwanted attention from the NSA and other intelligence agencies, including having your encrypted communications retained indefinitely.
- Using Tor makes web browsing *slow*. No, I mean *really* slow. Furthermore, QuickTime and other browser plugins are blocked because they pose too much of a security risk.
- Since Tor connections can go through so many different systems, Tor connections almost always have a high *latency*—the amount of time it takes for data from one end of a connection to reach the other. So you can forget about games and other applications that require fast responses.

Privacy is hard. Anonymity is *extremely* hard.

Shop Online Privately

I've already talked about steps you can take to protect the privacy of your web connection and your credit card information. As long as you're using an encrypted connection, any purchase you make online should be strictly between you and the vendor. Well, you and the vendor and the vendor's payment processor and your bank. And perhaps the fulfillment or shipping company. I can't tell you how to shop *anonymously* online, but most online purchases from reputable companies are already as private as they can be (which is to say, not very).

One common source of anxiety is giving out your physical address. If you're purchasing physical goods online, you have to provide a mailing or delivery address. Even if you're buying digital goods with a credit or debit card, you may still be asked for a billing address (which enables the vendor to calculate any applicable sales taxes and also helps to prevent credit card fraud—a good thing!). Other than renting a private mailbox, there's not much to be done about that. You may not have to provide your *home* address, but you will have to provide *some* valid

address at which you can receive statements. As long as you can do so over a secure connection, that shouldn't be anything to worry about.

Another common concern is the security of one's credit or debit card number, even over an encrypted connection. What might happen to it once it's in the vendor's hands? Is it safe?

I can't work up much fear about this, because laws and bank policies protect consumers against fraudulent use of a credit or debit card—or at least limit liability, as long as you report any suspicious transactions promptly. So, keep an eye on your bank statements and call your bank immediately if anything appears amiss.

If that's not good enough for you, I can offer a few other suggestions:

- Use Apple Pay. If you have an iPhone, iPad, or Mac, you can set it up to use Apple Pay, which works both online (if the site supports it) and at many brick-and-mortar stores, vending machines, transit conveyances, and other real-world locations. The great thing about Apple Pay, apart from its convenience, is that merchants never see your credit card number at all, so there's no chance that data will fall into the wrong hands. (Related, and potentially useful in situations where Apple Pay would not be, is the Apple Card—see the sidebar What About Apple Card?, ahead.)

  Google Pay works similarly, for owners of Android phones, in that it enables you to pay with a credit or debit card without revealing card's number to the merchant (whether online or offline). However, Google being Google, I can't help wondering whether my Google Pay purchases would be tracked and added to my profile in order to improve the company's ad targeting—something I'm keen to avoid.

- If an online vendor asks to store your credit card to simplify future purchases, say no. (Sadly, some store it without asking.) If you're using a password manager to enter credit card details, it's only a matter of a few clicks to provide that information anyway. However, even if you follow this policy generally, you might consider making exceptions for sites you shop from frequently, especially those with one-click checkout systems like Amazon and Apple.

- Use PayPal if that's an option. Now, I know a lot of people dislike PayPal for one reason or another, but one significant advantage is that it prevents vendors from seeing your credit card number (and, except for goods that must be shipped, your mailing address). Yes, you're trusting PayPal with a credit card or bank account number, but the merchant never sees it, and that limits your exposure.
- See whether your bank offers single-use credit card numbers for online purchases. Mine doesn't, but some do, and if you want to be sure a credit card number isn't misused after a single purchase, that could be an option. Alternatively, you can use the free privacy.com service to create virtual credit card numbers on the fly, or look for other comparable services.

Many other online payment systems exist—some of which go to even greater lengths to protect your privacy. But not all are as private as they may first appear. For example, Bitcoin and other cryptocurrencies promise anonymity, and yet we've seen numerous news reports about major cases in which law enforcement has nevertheless been able to trace cryptocurrency transactions, resulting in high-profile criminal convictions. Of course, if you're contemplating the use of any supposedly anonymous payment method to commit crimes, you should really…*not do that*. As a general rule, if a financial transaction requires cash-in-a-duffel-bag levels of anonymity, it's pretty likely not to be aboveboard, and I can't help you with those sorts of problems.

What About Apple Card?

Apple offers their own credit card, Apple Card, to customers in the United States. Part of the pitch for this card is it privacy focus. Apple doesn't know what you purchase with the card or how much money you spend, and even the issuing bank (Goldman Sachs at present, though that may change) promises not to use your purchase data for marketing or advertising.

You can use Apple Card either within the Wallet app on a supported device or in the physical world, thanks to a laser-etched titanium card. The physical card has no printed number, CVV code, or signature, and even when making online purchases at sites that don't directly support Apple Pay, you can easily generate new virtual card numbers to further protect your account's privacy.

The expert analyses I've read suggest that, as credit cards go, Apple Card is one of your better privacy bets, though on other metrics (such as its rewards program and interest rates), it's only so-so.

High-Risk Resources: Web Browsing

If you have to use the web while also under an extreme, specific privacy threat, here's what I advise:

- On an Apple device, enable Lockdown Mode.
- Use DuckDuckGo, StartPage, or Kagi for your web searches.
- Use Tor Browser if at all possible. If it's not possible, at least use a privacy-friendly browser such as Vivaldi, crank all its privacy settings up as high as they'll go, and install an excellent ad blocker.

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.

- **On the recipient's end:** Everything that's true on your end is also true on the recipient's end, with the additional complication that you have no control at all over what the recipient does with a message received from, or sent to, you. And, if the recipient uses multiple devices or services for email, your message may be on any or all of them.
- **In backups:** You, the recipient, and whoever runs email servers that process your messages most likely back up your data to one or more other locations such as local hard disks and cloud storage. (Good for you! Backups are mighty important.) Those backups may be encrypted, but if they aren't—or if someone with access to the media on which the backups are stored can crack or bypass the encryption—that's another way your email message could be read.

This isn't even an exhaustive list, but I hope that it explains Adam's contention that complete privacy of email messages between you and another party is little more than wishful thinking. Someone who wanted to know what you sent or received by email would have many potential ways to do so.

Note: There's yet another risk: accidentally sending confidential email to the wrong recipient (or even to a mailing list)! I've done it myself, and I've also received confidential email addressed to me by mistake. Double-check the address(es) before clicking Send!

None of this means someone *is* reading your email. I'd wager that the overwhelming majority of email messages are never read by anyone other than the sender and recipient. But *machines* absolutely could be reading your email, for reasons such as training AI or looking for keywords that can be used for marketing. So, if you discuss anything sensitive by email, you should be aware that the possibility exists that it's not private. And, if the contents of a message are such that someone may have financial, legal, or political motivation to read it, the odds of exposure increase. Unfortunately, because email messages are out of your control the instant you hit Send, it's impossible to quantify the risk.

Email can compromise your privacy in other ways too, even if you never send a single message. I discuss that issue ahead, in Mind Your Incoming Email.

Reduce Email Privacy Risks

Now that I've told you how hopeless complete email privacy is, I want to cheer you up a bit by talking about steps you can take to reduce—not eliminate—the potential for email-based privacy threats.

First, I want to tell you about some of the risks of your *incoming* email in general and what you can do about them. Then I turn to the messages you send (along with their responses). You don't want your email messages to fall into the wrong hands, and in this case, you protect your privacy by increasing security. The more of these things you do, the fewer opportunities an attacker will have to read what you send and receive. In most cases, they'll be enough. And since you now understand that email privacy can't be perfect, you'll at least be able to make smarter decisions about what should and shouldn't go in an email message.

Mind Your Incoming Email

Did you know that merely *opening* email—even if you don't reply, or send new messages yourself—can have undesirable privacy implications? It can. I'd like to tell you about a few of them, and suggest some ways to reduce the risks.

Spam

Unsolicited commercial email messages have been a thorn in the side of every email user for decades. Most of the time, they're just annoying—we delete them and move on, or better yet, use an email provider or third-party spam filtering app or service that zaps most of them automatically. But what do these irritating messages have to do with your privacy?

Well, many of these messages contain links to remote graphics, and it's easy for senders to customize those links such that merely loading the

image informs them that you've opened and read their message—something you might not want anyone (especially spammers) to know. Why not? It confirms that your email address is valid and active. But not only that! Loading images reveals information about your device and your IP address (and thus something about your physical location). In some cases, loading remote images can do other nasty things too, such as setting or reading cookies (if you check your email in a browser) or even downloading malware.

The surest way to avoid this problem is to configure your email program *not* to load remote images automatically. If you receive an email message with images you want to see, you can click a button to override that preference and display them, but you'll avoid the automatic disclosure of your personal information to people who shouldn't have it.

Each email app and service has its own way to do this. For example, in Apple Mail for macOS, go to Mail > Settings > Viewing and uncheck "Load remote content in messages." You can also read how to do this in Outlook for Windows or Mac, or Gmail; for other email apps, a quick glance at the documentation or a web search should point you in the right direction.

Tracking Beacons

Tracking beacons (or tracking pixels) are a notable subset of trackable remote images in email messages. They can do all the same things I mentioned above, because they're also links to remote graphics, except they're *invisible*—in most cases, they're tiny, 1-by-1-pixel GIF files. I list them here separately because, even though they can be (and often are) used in spam messages, they're also used regularly for less sinister purposes.

Tracking beacons let the sender know whether (and when) you've read their message. This is helpful for marketers, of course, who are trying to gauge the effectiveness and reach of their email campaigns. But it's also useful for ordinary people like you and me who might be worried that their messages are getting lost or swallowed by spam filters, and want to confirm that they made it safely to their recipients. And it's as

likely as not that someone using such a beacon only discovers (or even cares about) that one piece of information—did they open it or not?—and not other details such as your IP address and location.

So although I consider tracking beacons relatively benign when they appear in non-spam messages (and I've even used them myself on occasion), I would not blame you at all for wanting to avoid letting them track you—or at least, exercising control over when they're permitted to load. Since tracking beacons are just graphics, you can disable them using the same steps I provided above under Spam. If you're an Apple user, you can also use Mail Privacy Protection.

Phishing and Malware

All of the categories I've mentioned so far are privacy risks that require you to do nothing more than open a message, something most of us do without thinking. But there are additional threats that could face you if you take action on the contents of a message. For example:

- **Phishing:** I've mentioned phishing in a few other contexts in this book. Basically it's the effort to trick you into revealing private information—most often, the username and password protecting something of value. In a typical case, an email message convinces you to click a link, which takes you to a site that looks very much like that of your bank, or PayPal, or eBay, or Apple or whatever (see Go to the Right Site). But it's fake, and once you fill in your credentials, the bad guys have them—they'll use them to log in to the real site and cause all kinds of havoc.
- **Malware:** I've also mentioned malware quite a few times (see, for example, Avoid Malware). It's nasty stuff with seriously bad privacy implications. And email is one of the ways it spreads—either as an attachment (perhaps one disguised to look like a PDF, Word document, or something else innocuous) or as a link.

How can you avoid these threats? Here are some tips:

- **Don't click links in email messages if you're not sure of their source.** I wouldn't say to avoid clicking links in email messages altogether. Sometimes you have to do that to confirm your

email address for a new account, for example, or sometimes a person or company you trust will send you a message about a new product or service you might be interested in, and of course there'll be a link to that. But…be suspicious. If in doubt, don't click. (On a Mac or PC, you can usually hover over a link to see its destination before you click it, and if the destination appears to be a shortened URL, a service like unshorten.it can tell you its ultimate destination.) For more on this topic, see the sidebar Email Links: A Case Study, ahead.

- **Don't open attachments if you aren't positive that the sender is trustworthy and the attachment is something you're expecting.** Most of all, don't open suspicious attachments that are executable files (such as `.exe` files on Windows or `.pkg` files on macOS).
- **Use a password manager.** I discussed this in the sidebar Choosing Better Passwords, among other places. If you do accidentally go to a phishing site and you use your password manager to fill in your credentials, it most likely won't work, because it'll be able to tell that the site you're on is not the same one where you set up those credentials in the first place. That's an extra line of defense against phishing attacks.
- **Use antispam measures.** Whether you use an email provider with its own antispam system, a third-party service, or an app on your Mac or PC, do *something* to enable automated scanning of your incoming mail to look for spam, phishing attempts, malware, and other undesirable crud.

Email Links: A Case Study

A friend of mine (who, um, did not read this book) told me about an experience she'd had. Here's an abbreviated (and annotated) version of the story.

My friend received an email message that appeared to be from the U.S. Postal Service. Although she was suspicious, since she had an account with the USPS and often received legitimate mail from them, she decided to go ahead and click the link in the message. *(The message and its link were not in fact legit, as she would have discovered from hovering over the link and checking the message headers.)*

After she clicked the link, an alert appeared on her computer warning that she had a malware infection *(possibly true, but only because she just installed it by visiting a malicious site)*, and that she should telephone Microsoft to resolve the problem. *(Microsoft doesn't operate like that; the message was fake.)*

She called the number, thinking she was talking to Microsoft. *(She wasn't.)* The person on the phone asked for permission to share her screen and control her computer, which she granted. *(Obviously, she shouldn't have done that.)* The fake Microsoft rep then made some windows appear that seemingly "proved" that she had a malware infection. *(Again, maybe true…or maybe just about to be true.)*

At this point, the rep proposed the solution of selling my friend some very expensive anti-malware software (to the tune of $300), which she agreed to, and the rep installed it remotely. *(The software may have been legit, if overpriced, but more likely, it was itself malware.)* The problem having thus been "solved," the rep ended the call. *(In fact, the problem was just beginning.)*

My friend couldn't tell what the remotely installed software was doing. Even if it was real anti-malware, she got scammed into paying for it based on a phony alert. If it wasn't real, and I don't think it was, she paid to have her computer infected with software that could spy on her, monitor her keystrokes, and worse. So I had to recommend that she spend even *more* money by taking her computer to a reputable shop and having it scanned for malware independently.

Of the many morals one could draw from this story, the one I want to highlight is: *don't click links in email messages unless you're absolutely certain you know where they go.*

Log In and Transfer Email Securely

In earlier editions of this book, I devoted several pages to explaining the details of configuring your email client so that it uses encryption when communicating with your mail server—both for logging in (encrypting your password) and for transferring messages. To be sure, both of those factors remain important.

At the same time, both elements are also standard, default settings across nearly all modern email servers and clients. (If your email client is set up to use TLS/SSL to connect to any given server, then both your login credentials and the email messages in transit when sending or receiving are encrypted, though they're not necessarily encrypted while sitting on the server.) I don't want you to waste time and effort figuring out settings that are almost certainly already correct.

One exception might be if you've been using the same email account for decades, transferring settings from one computer to another without ever reviewing or updating them. If that description applies to you, it's conceivable that your email account is set up in a less-than-secure way. In that case, I recommend reviewing your email provider's current setup instructions, comparing them to the settings in your email app, and making sure they match.

Use Burner Addresses

Another aspect of email that can affect your privacy is your email address itself, and in some cases you may want to take additional steps to hide it by using a *burner address*, also known by many other names ("temporary," "disposable," "obscured," and so forth). Regardless of terminology, it's an address that enables you to receive messages while preventing the sender from knowing your true email address.

Let's say my email address is `joe@takecontrolbooks.com` (which is true, at least for one of my many accounts). By knowing nothing other than that address, someone can make the reasonable assumption that my name is Joe and that I work for, or am in some other way associated with, Take Control Books. Those two pieces of information aren't exactly a secret, but they do give people information that could be used to learn much more about me, and to make assumptions about my

interests, location, beliefs, and more. If your email address includes your first *and* last name, that forms an even closer connection to you personally. And although an address that ends with, say, `@gmail.com` or `@outlook.com` does not, by itself, reveal any further specifics about you, an `@icloud.com` address indicates with rather strong certainty that you're an Apple user, while an address that ends in a personal domain (say, `@joekissell.com`) not only reinforces who you are but also suggests you have at least a bit of technical know-how.

Even an arbitrary email address, such as `g9n2q8o0@made-up-domain.com`, while conveying little information by itself, forms part of your digital identity and can be used for profiling and tracking. Any time you enter that address in a web form, use it to make a purchase, or sign up for an account with it, that information can be sucked into the databases of advertisers and data brokers. If even once you included your real name, address, phone number, or other personally identifying information along with that address, you've pretty much guaranteed that Big Data knows exactly who you are and what you're doing when you use it.

These are just some of the reasons for using burner addresses. When you sign up for an account or make a purchase with a burner address, the entity on the other end knows only that *someone* did that, but not that you're the same person who matches a profile they already have. It essentially fragments your digital footprint by keeping certain portions of it isolated from the others.

Although each of the many implementations of burner addresses works slightly differently, in general, the process goes like this:

1. You use the service to generate a random email address.
2. You enter that burner address when asked for your email address online.
3. Whenever someone sends email to the burner address, it's forwarded automatically to your real address. (Sometimes you can freely reply and the reply is automatically sent from the burner address,

while in other cases you have to jump through extra hoops to make sure the reply doesn't reveal your actual address.)

4. If the burner address starts receiving spam, or if for any other reason you want to prevent anyone from getting through to you at that address, you can delete it while keeping your real email address intact. (That's the "burner" or "disposable" aspect.)

I should caution you that using a burner address does not in any way guarantee anonymity or protection from tracking. A determined attacker could still potentially learn useful things about you (or even uncover your real-life identity) from a burner address, depending on which service you use, how careful you are to use each address in one location only, and—this is a big one—whether you ever provide someone with another piece of personally-identifiable information at the same time. (For example, if I use a burner address but my actual phone number, it's trivial for the other party to figure out who I really am.) You also have to assess how trustworthy the service provider is: after all, they do know your real address and could possibly disclose, sell, or inadvertently leak it.

Even so, burner addresses can be useful in certain situations:

- You have a specific reason to distrust a person or site.
- You think there's a high probability of receiving spam or other unwanted email if you were to provide your real address.
- You want to contact a journalist confidentially.
- You're dating people you don't know and want a layer of protection against stalking.
- You want to create an account or make a purchase of a sensitive nature, with as little connection to the real you as possible.

In my opinion, burner addresses are best used sparingly, because they create additional work for you (and an additional potential failure point) while solving what is in most cases merely a hypothetical problem. I don't want to convey the impression that if you *ever* use your real email address, you're taking a huge risk, or that from now on you

have to use a different address for every site you visit. That sort of attitude strays into paranoia. But when an appropriate situation arises, it's good to know that you have this option.

Some example providers of burner addresses:

- addy.io
- Apple's Hide My Email and Sign in with Apple services
- Burner Mail
- DuckDuckGo Email Protection
- Guerrilla Mail
- Maildrop
- Proton Mail's Hide-my-email aliases

IMAP vs. POP Privacy Implications

IMAP and POP are the two most common protocols for delivering incoming mail from servers to clients. I've long been an advocate of IMAP, which typically keeps the master copy of each received, sent, and filed message on the server but synchronizes these messages with each of your local clients. Compared to POP, which usually deletes messages from the server after you download them, IMAP makes it much easier to use more than one device for email. (For more on POP and IMAP, including common misunderstandings about IMAP, see my article FlippedBITS: IMAP Misconceptions.)

An IMAP privacy concern is that if your password were compromised, someone could see *all* your email messages, not just a handful of recent messages as in a POP account. A combination of an excellent password and (if available) two-factor authentication (see the sidebar About Two-Factor Authentication) reduces this threat considerably.

I've also heard people say they prefer POP for privacy on the theory that the less time messages are stored on the server, the lower the risk that an unauthorized person might read them there. However, I am skeptical that downloading messages from a POP server and deleting them on the server provides significantly better privacy. If, for example, a government agency had a black box in your email provider's data center capturing all email, it would catch incoming POP messages before they were deleted. And, even though POP messages may be deleted from a server after they're downloaded, they could be backed up or cached without your knowledge. If you think of POP as a magic bullet to circumvent snooping, think again.

Meanwhile, it's often possible to change the settings in an email client that's using IMAP so that only some messages (such as those in your inbox) are automatically synced. And that, in turn, could increase your privacy if someone gets access to your device, because the messages wouldn't be sitting there waiting to be read. (You would, however, want to change your password in the event of loss or theft to prevent someone else from connecting to your IMAP account and downloading more messages.)

Email Your Doctor, Accountant, or Lawyer Privately

Members of certain professions, such as doctors, accountants, and lawyers, regularly discuss highly personal and sensitive topics with their clients. Given everything I've said about the privacy risks of email, you may be wondering whether you can communicate safely with such people by email. The short answer is maybe.

Privacy laws have led to the widespread adoption of secure web portals for communications with doctors and with some financial institutions. The way these work is that both you and the person on the other end connect to a secure website using a username and password, and all email remains solely on that site—it works very much like any other webmail service, except all messages are stored encrypted on the server, and are not accessible via POP or IMAP (or to Gmail, Outlook.com, or other email services).

In some cases, a secure web portal may send you a conventional email message to let you know that a secure message is waiting on the server, and that you should log in to read it. That may seem awkward, but there's a good reason for it: sending the message directly to you outside the secure system may be not only risky but also illegal.

Confusingly, rules and policies governing secure email vary by country and profession, and they're always changing. When I lived in France from 2007–2012, I regularly exchanged ordinary email messages with my doctor, but my bank pushed me to use a web portal. Here in North America, my doctor will only use a web portal, but my banker sometimes sends me conventional email.

If you want to send confidential email to a doctor, accountant, or lawyer, ask whether they have access to a secure web portal or a comparably secure method of communication. If not, a phone call might be a better choice. And, if you're a professional in one of these sensitive occupations and don't use a web portal to communicate with clients, I strongly recommend reviewing the relevant laws and professional conduct standards for your area to determine your best course of

action. Be careful sending confidential information over ordinary email—you could be exposing yourself or others to legal liability.

Encrypt Your Email

Even if you use TLS/SSL with all your email accounts, you've seen that messages are unencrypted while they sit on various email servers, and often for their journey from one server to another. The only way to be sure they're private from end to end is for you as the sender to encrypt them, and for the recipient to decrypt them.

Encryption, like TLS/SSL, is a great idea, and in an ideal world, perhaps all messages would be encrypted all the time. In a moment I'll mention a few ways you can go about encrypting messages if you choose to. But first, let me try to talk you out of it. That's right: I think encrypting email is a less-than-optimal solution for most people, most of the time. Here's why:

- Once the recipient has decrypted your email message, anything could happen to it, and it's entirely out of your control. A message may stay private all the way to Mr. X, but if he's not careful (or if his computer or phone is stolen or hacked), your message could still get out.
- Configuring an email client to encrypt messages can be (depending on the platform and software) a cumbersome process. Once you've done that, encrypting individual messages is usually simple, but requires that your recipients use the same type of encryption, and set up everything correctly on the other end. Even then, in some cases you must go through extra steps to obtain a public key or certificate from the other person before you can send secure email; in other cases, both parties must find some way other than email to swap passwords. You wouldn't want to go through this bother for every message you send.
- Although encryption protects the *contents* of your messages, it doesn't protect their *headers,* which means that someone with access to your encrypted email while in transit or on a server could

still see the message subject, sender and recipient's email addresses, date and time, and other information that may itself be private.

- As things currently stand in the United States, the NSA can retain indefinitely any encrypted email messages it happens upon, presumably to help the agency learn how to break that encryption. Unfortunately, the very fact that you encrypt messages—regardless of their content—may mark you as a suspicious person subject to more in-depth monitoring. Encrypting email messages not only draws attention to yourself but could also mean that any messages that are intercepted will be kept until the NSA can figure out what they say or decides it's not worth knowing. Other nations may have even more aggressive policies regarding encrypted email.

Those qualifications aside, if you still want to go for it, there are three main techniques you might use:

- **S/MIME:** Almost all modern email clients, including Apple Mail on macOS and iOS, Outlook, and Thunderbird, support an industry standard called S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME uses a form of public-key cryptography: you give me a public key (in the form of a file called a certificate) that I use to encrypt a message I send you, and then only you can decrypt it with your corresponding private key. To reply to me, you reverse the process, encrypting a message with my public key; I decrypt it with my corresponding private key.

  Before you can use S/MIME, you must obtain the necessary certificates and install them on your device; it's a tedious and non-obvious process. (I describe how to do this in Apple Mail—for both macOS and iOS—in *Take Control of Apple Mail*.) Your correspondents must also use S/MIME, and you'll need their public certificates to send them encrypted messages.

- **PGP/OpenPGP/GnuPG:** The commercial PGP (Pretty Good Privacy), owned by Symantec, and the compatible, open-source OpenPGP standard and GnuPG (Gnu Privacy Guard, also known as GPG) software represent another flavor of public-key cryptography. Conceptually, PGP (including OpenPGP and GnuPG) is roughly

comparable to S/MIME (in fact, newer versions of GnuPG also support S/MIME), although the implementation is different.

You'll typically need to install extra software on your device to use PGP, and it may not be available for your favorite platform or version. However, the process of obtaining public/private key pairs is simpler than with S/MIME, and it optionally uses *keyservers*, which let you obtain someone else's public key by looking up a name or email address rather than having to contact that person first. Although most webmail services still don't offer encryption of any kind, you can use a browser extension for Chrome (and other Chromium-based browsers) or Firefox called Mailvelope to add PGP capabilities to nearly any webmail service. In addition, webmail providers Hushmail and StartMail directly support PGP—and there's an additional web-based option in the next bullet point.

Note: Hushmail offers a way to send encrypted messages to non-members, though this requires Transferring Passwords Out of Band.

SecureMyEmail, an encrypted email service from WiTopia, lets you use your existing email address and provider. It uses a custom app (available for macOS, Windows, iOS/iPadOS, or Android); plugins for Apple Mail and Microsoft Outlook are supposedly in the works—but the company has been saying that since at least 2017, so I wouldn't hold my breath. By default, messages sent to people who aren't already SecureMyEmail subscribers will prompt them to sign up. But the service uses PGP behind the scenes, so it's also compatible with existing PGP keys and tools. The service costs $29.99 per year and is also available bundled with a VPN service.

Note: You can look up my PGP public key by name or email address in any keyserver (such as the MIT PGP Public Key Server) if you want to use PGP to send me encrypted messages. I won't reproduce it here because it would go on for pages.

- **Proprietary encrypted email:** The beauty of S/MIME and PGP/GnuPG is that they're industry standards that anyone can adopt and that can be used by most email apps. The downside is that they're

complicated to set up and often frustrating to use. An alternative is to use a third-party service that handles all the messy details in the background and presents you with a lovely, straightforward interface, but requires that both parties use the same system. I'll give you two examples:

- ProtonMail is a Swiss service that offers PGP-compatible, web-based encrypted email, as well as iOS and Android apps and (for paid users only) an app called ProtonMail Bridge that enables the service to work with conventional IMAP and SMTP email clients such as Apple Mail, Outlook, and Thunderbird. If you're sending email to another ProtonMail user, it's encrypted automatically. When sending email to someone without a ProtonMail account, you can check a box to encrypt it and supply a password; the recipient receives a message with a link to open the message on the ProtonMail website after entering the password. (Of course, this means you must find a way to get the password to the recipient securely; see the sidebar Transferring Passwords Out of Band, ahead.) A basic account is free; paid accounts (starting at $4.99 per month or $47.88 per year) add features and storage space. You can send me email via ProtonMail at joekissell@protonmail.com.

- Tuta (formerly Tutanota), based in Germany, is another free, web-based encrypted email system that also offers Mac, Windows, Linux, iOS, and Android apps. Much like ProtonMail, you can send encrypted messages to other Tuta users, while messages to others require a password (which must be communicated separately) for decryption. A premium account, which costs just €12 per year, adds quite a few features (including aliases and custom domains). To contact me via Tuta, send email to joekissell@tutamail.com.

- **Encrypted attachments:** A somewhat simpler, lower-tech approach is to send an ordinary email message containing an attachment that's encrypted; inside the attachment is the private content you want to transmit. There are numerous apps (many of them free) for all platforms that can encrypt files or folders; search your fa-

vorite app store for ideas. However, there's just one problem, which is that the recipient needs the password, and you can't send that by email! The sidebar ahead discusses what to do.

As an alternative for sending the occasional encrypted file, you can use a messaging app that supports end-to-end encryption; see Improve Your Real-Time Communication Privacy.

Transferring Passwords Out of Band

When you need to send someone information using a different communication method than the one used for the main content of the message, that's called *out-of-band* communication. Even if the out-of-band channel isn't secure, the fact that you're conveying the password by a different means than the message itself reduces the likelihood that the same person will intercept both pieces of data.

For example, say you've sent me an encrypted file and you need to tell me the password. How might you do that? Here are some ideas:

- **In person:** The best and most reliable method, if practical, is to tell me the password face to face.
- **By phone:** Phone calls can be tapped or overheard, but it's harder to do and may be trickier legally than eavesdropping on email.
- **By chat or private message:** Exchange the password with an encrypted text or voice messaging system such as Skype (but only using its Private Conversation feature, as regular Skype calls are known to have a government back door), Apple's iMessage, Signal, WhatsApp, or another service that offers end-to-end encryption (some are listed ahead in Understand the Privacy Risks of Real-Time Communication). As with all electronic communications, there are no guarantees, but they're safer than email.

Whichever method you use, you can enhance its security considerably by using shared knowledge. If you know the recipient well, you may be able to construct a story that implies the password without spelling it out. For example, "The comment that girl next to you at the concert made about your shirt, plus your sister's age when we first met."

Send and Receive Email Anonymously

In rare cases, email privacy requires anonymity; revealing your name, your real email address, your IP address, or other personal facts could get you in trouble. I'm thinking, for example, of a confidential source contacting a reporter, an informant telling the police about suspected illegal activities, or someone making politically hazardous statements. In such situations, you may need to disguise the source of the message in such a way that it can't easily be traced back to you specifically.

Numerous services exist for just such a purpose. A quick web search turns up options that let you send anonymous email with a simple web form (such as Anonymous Email). With some research you're bound to find many others, including one that suits your particular needs.

However, as usual, I must caution you to read the fine print. Some of these sites log your IP address or other details in such a way that messages could be traced back to you if necessary, and no matter how secure a site claims to be, vulnerabilities could exist that might expose you. And be aware that textual analysis could provide clues to your identity based on word usage and writing habits. Tread carefully if you feel you must use such a service.

Use Email Alternatives

Regardless of encryption or anonymity, you may encounter situations in which email doesn't make sense as a means of communication. In particular, if you're worried about something you write being found on someone else's computer in the future, email is not a good choice.

In the sidebar Transferring Passwords Out of Band, I mentioned several ways you might send someone the password for an encrypted file; all the same methods can be used as alternatives to email if you have something to say that you simply can't take any chances with. And I go into more detail about one such category in the next chapter, Talk and Chat Privately.

Another option I should mention is the self-destructing digital message. Although these take various forms, the general idea is that you send someone a link to a message on a website, or using a mobile app—and once viewed, that message is visible for only seconds or minutes, after which time it's permanently deleted. Although such systems aren't foolproof—the recipient might, for example, take a screenshot of the secret message before it self-destructs, or use file recovery software to undelete it after the fact—they do reduce the risk that a private message will later be discovered on someone else's device, at least by technically unskilled people.

I found many such services and apps on the web, although I haven't tried them personally, so I can't speak to how effective, secure, or easy to use they may be. A few examples:

- SafeNote
- Self-Destructing-Email
- Snapchat

High-Risk Resources: Email

If you have reason to believe you may be personally targeted for surveillance or other mischief, you should take stronger measures to protect your email—and you should do this for *all* messages, not just ones you're particularly worried about. The most comprehensive approach would be to sign up with an encrypted email service such as ProtonMail, make sure everyone you correspond with has the new address for that service, and then completely sign out of all other email accounts on all your devices.

Of course, that's going to cause problems. You'll still get tons of legitimate email sent to other addresses of yours, which you then won't see! (Some of those messages could even be extremely important to your privacy, such as password resets and second-factor login codes.) You could check those remaining accounts, as needed, using webmail while connecting via Tor (see Browse Anonymously). That is, of course, inconvenient, but if your safety is at stake, you do what you have to do.

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

- Signal
- WhatsApp
- Wire

Like iMessage, these services are proprietary, requiring that the people you chat with have accounts on the same service. (For another type of secure messaging, see the sidebar Using Keybase for Identity Verification and Chat, ahead.)

Note: WhatsApp is owned by Facebook, which, as I've discussed (see Learn About the Facebook Problem), is not exactly known for its stellar privacy practices. However, WhatsApp itself is based on the same very secure infrastructure that Signal uses, and, for consumers at least, should keep the *contents* of chats private from Facebook. But nothing else.

- Communication that takes place entirely over the internet (for example, Skype-to-Skype calls or FaceTime chats) or entirely over analog phone lines is probably safer than communication that crosses between the two (such as using Skype or a VoIP service to call a landline phone) because calls that traverse multiple networks have more potential points of interception. However, even if you have an analog phone line, you should be aware that the signal is likely analog for only a short distance, as telephone companies routinely convert the signal to digital somewhere along its path.

Security in iMessage and Other Apple Services

Earlier, I discussed Apple's *privacy* measures (see Discover Apple-Specific Privacy Features). But if you're curious to learn exactly what *security* measures Apple uses with iMessage, iCloud Keychain, and other services, you can find them in the PDF Apple Platform Security. For a less technical summary of the iCloud Keychain portion of this document, read Rich Mogull's TidBITS article How to Protect Your iCloud Keychain from the NSA.

And, to learn much more about how iCloud Keychain works and how to use it, see my book *Take Control of iCloud*.

Using Keybase for Identity Verification and Chat

A free web service (and associated app) called Keybase enables you to do a variety of tasks:

- Prove your identity in a variety of ways—for example, you can prove that a certain Facebook or X account, or a certain web server, belongs to you—or confirm someone else's identity.
- Publish your PGP public key, or find someone else's public key.
- Participate in chats that are encrypted from end to end. (For more on this topic, read Glenn Fleishman's Macworld article Keybase offers encrypted chat where you control all the pieces.)
- Share files privately (in which case they're encrypted) or publicly (with proof that they really came from you).
- Use PGP to encrypt messages in a web browser (which you can then send manually by email, instant messaging, or other means).

Keybase has a bit of an identity problem in that it's unclear to the average person what it actually *is*. But for those of a geekier disposition who want a way to do the above tasks, Keybase is well worth a look. (Needless to say, you can contact me using Keybase too—go to https://keybase.io/joekissell.)

Improve Your Real-Time Communication Privacy

If you have money to burn and a powerful need for a "secure line," you can buy secure telephones (landline) or crypto phones (mobile) with built-in hardware encryption. There are also various hardware and software products (for example, Silent Circle) that can work with existing phones to achieve the same effect. But end-to-end encryption means both parties will need interoperable equipment or software.

For the purposes of this book, I'm assuming you don't need such a heavy-duty solution. For improving your day-to-day privacy in real-time communication, I suggest the following:

- **Read the privacy policies.** Your mobile carrier, ISP, VoIP provider, instant messaging service, and other such companies has boring pages of legalese, but you should at least be able to scan them to see if the services encrypt your data, and under what circumstances they may share your information with others.
- **Use end-to-end encryption when available.** Apps mentioned earlier in this chapter—such as KeeperChat, Messages (using the iMessage Protocol), Signal, WhatsApp, and Wire—offer end-to-end encryption that the providers themselves apparently can't crack. Use one of those if possible. If not…
- **Consider obscure products.** If you're unable to use end-to-end encryption, you can gain a small advantage by using an app that isn't one of the major players. After all, hundreds of millions of people use Skype, making it an attractive target for both official surveillance and hackers. Newer and less-popular communication services—more of them are popping up all the time—might not be large enough to attract that sort of attention. Of course, they also may not have the expertise or resources to engineer or operate a high-quality service…or may not be what they appear to be.
- **Favor higher-bandwidth communication.** All things being equal, if circumstances permit, choose video before audio, and audio before text—simply because anything other than text makes it less convenient (and more expensive) to capture, store, and analyze your conversation (and all the more so if it's encrypted). Remember, none of this means audio or video is entirely safe from snooping, but the odds are more favorable than when using text-based communications.

High-Risk Resources: Talk and Chat

If you must communicate with someone by voice, video, or text and serious risks are involved—someone's life, your vast fortune, or the fate of the free world—you should take extra precautions.

Of course you'll want to use encrypted communication, but in the most extreme cases, you might want to add more layers of protection:

- On an Apple device, enable Lockdown Mode.
- Sign up for a completely new account with whatever service you plan to use (or even sign up with a service you've never used before). The less the bad guys know about the means you use to communicate, the more difficult it will be for them to attack you.
- Activate a VPN on whatever device you're using to communicate.
- Always use a service (or a feature of a service) supporting end-to-end encryption between your device and the devices of the people with whom you are communicating.
- If you're using a web browser, as opposed to an app, to communicate, use its private browsing mode—or, better yet, use Tor Browser.

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

to advertisers. Unlike regular cookies, supercookies can't be blocked or deleted, because the carrier inserts these unique identifiers between the time a request for a page leaves your device and the time it's sent to the server.

At the time, AT&T claimed they had only tested the feature briefly and were no longer using it. However, whether using that specific technology or not, AT&T still, by default, collects "Customer Proprietary Network Information" (CPNI) and uses it for marketing purposes; it's opt-out only. Verizon, meanwhile, tried to spin supercookies as a beneficial feature, but under public pressure, finally agreed to let its customers opt out. Then, after being fined by the FCC, they were required to obtain consent from customers before sharing supercookie data. More recently, German telecom companies such as Vodafone and Deutsche Telekom were found to have been using supercookies of their own.

There's no guarantee that other carriers aren't using technology like supercookies, and the nature of these tracking mechanisms makes it nearly impossible for an ordinary user to know whether it's happening. And, there's nothing special about mobile carriers in this regard; any internet provider could use a mechanism like this to track its users. Unfortunately, this lack of transparency means there's nothing you can do to protect yourself preemptively—except not connecting to their services—but if you find that a provider you use is employing something like supercookies, you'll know to opt out immediately.

Granting Apps Access Permission

Third-party apps on your mobile device may ask for permission to access your contacts, calendars, location (see the next topic), and other private information for various reasons. In some cases, such requests are legitimate—for example, if you're using an VoIP or instant messaging app, you may want it to be able to look up your contacts' phone numbers or email addresses.

However, apps have been known to overreach, requesting access to data that's truly none of their business. In one example, mobile games

were found to be using devices' microphones to determine what TV shows the users were watching—even when the games weren't being played. And period tracker apps have been known to share the information that the user is potentially pregnant with advertisers who then bombard them with ads for prenatal vitamins and baby supplies. There's seemingly no end to how clever and creepy app developers can get when it comes to collecting and monetizing your data. Once an app has your data, there's nothing stopping it, in principle, from sending that data to the developer, to advertisers, or to other parties.

My advice, as always, is to be suspicious. Your default response, when an app asks you for permission to access private data, should be to say no; if that causes problems later, you can always change your mind. If you're unsure which apps can currently access what, it doesn't hurt to check. On an iPhone or iPad, go to Settings > Privacy & Security and then tap a category, such as Contacts or Calendars, to specify which apps can access that type of data. For Android devices, see Change app permissions on your Android phone. For iPhones and iPads, refer back to Privacy Nutrition Labels, App Privacy Report, and Location Tracking Protection.

Tip: Your Contacts and Calendars apps probably have a Notes field for each contact or event. Be careful what you put in this field—it is almost certainly not encrypted, and is potentially available to any other app that can access your contacts or calendars.

Location Awareness

Mobile phones and other devices that use wireless data are *constantly* connected to cellular networks—even when you're not using them. So, the mere act of carrying a mobile phone or other device that uses cellular data networks reveals your approximate physical location to the carrier (because the carrier knows which cellular tower(s) your device connected to) and updates it in real time. Depending on the circumstances, more exact details (including GPS coordinates) might be transmitted. Location awareness is part of the very nature of cellular

communication: cellular networks can't operate without it, and if you use a cell phone, you can't avoid it.

That wouldn't be terrible if cellular providers guarded your location data carefully. They don't—in fact, the three biggest carriers in the United States sell location data pretty freely, and you would be shocked at how much detail about people's locations is readily available. When I wrote the previous edition of this book back in 2019, it looked like U.S. carriers were starting to clamp down on this practice. But as recently as April 2024, the FCC fined the four largest U.S. carriers (AT&T, Sprint, T-Mobile, and Verizon) almost $200 million for selling their customers' location data. You should absolutely not assume those penalties are large enough to deter this practice! And even if they did, that would affect only customers in the United States.

Realistically, *most* people have little to fear from that location data, except for a greater number of location-sensitive ads. (The wealthy, famous, and powerful have considerably more at stake here.) A much bigger privacy concern, in my opinion, comes from your mobile apps, many of which will ask your mobile device for its location in order to provide maps, driving directions, traffic reports, real estate listings, weather forecasts, or any of countless other pieces of information. The photos and videos you take are almost certainly geotagged with your location when you took them. There are also the Find My features of iPhones and iPads (and comparable features on other platforms), which let you track your own device or someone else's (with their permission) in near-real time. And the list goes on.

All these things are useful, and most people have no reason to turn them all off en masse. But you can't know for certain what happens to that location data. Maybe the app developer uses it for something sinister, maybe they resell it, or maybe it falls into the wrong hands through hacking or other means, and someone discovers your location who has no business knowing it.

So, consider curtailing apps' privileges to know your location if:

- You need to keep your location secret for personal or professional reasons.

- You think you might be individually targeted for a crime (including property crimes when someone can tell you're away from home).
- You find location-based advertising creepy and intrusive.
- You can't think of any valid reason a particular app should know where you are.

The exact procedure for restricting apps' access to your location data varies by operating system and version. On an iPhone or iPad, go to Settings > Privacy & Security > Location Services. There, you can either turn off Location Services entirely or restrict it on an app-by-app basis (flip back to Location Tracking Protection for details). You can also tap Share My Location to control whether and with whom Find My shares your data. For Android devices, see How to Turn Off Google Location Awareness on Android Mobile.

Another aspect of location awareness involves your device's Wi-Fi MAC (media access control) address, which is continually broadcast when Wi-Fi is enabled. Because this address is unique to your device (at least for a limited time), any receiver within Wi-Fi range can determine your device is nearby, and, depending on your actions or what information has been collected previously, could associate that address with you personally. Even though recent versions of iOS, iPadOS, and Android use a technique called MAC address randomization to change this address regularly (which should reduce the possibility that you'll be personally identified), that feature was significantly broken and exploitable until very recently. The only way to be certain no one can identify you is to turn off Wi-Fi: I don't generally recommend that because of the significant inconvenience it could cause, but you may want to consider turning off Wi-Fi in locations where you're not using it.

Your device likely also has Bluetooth, a short-range radio to connect wirelessly to items like keyboards, earphones, and speakers. That's great, but Bluetooth is also used to track mobile devices in an increasing number of retail and public spaces. Technologies like Bluetooth beacons (ironically pioneered by Apple, in 2013) send messages to nearby devices. The idea is if a user has the retailer's mobile app

installed, beacons can inform the user about products or send personalized offers or messages. Of course, these beacons also tell the store operator when and where a customer turned up. (And if this sounds creepy, think about the impact for store *employees.)* But device owners don't need apps to be tracked through a space: Bluetooth proximity detectors like beacons can pinpoint other Bluetooth devices to within centimeters, and—just like other digital marketing profiles—those data can be compiled and used to more specifically identify groups and even individuals. If this concerns you (or you are in a high-risk situation), don't use retailer or "loyalty" apps that rely on Bluetooth beacons, and consider turning off Bluetooth before entering retail and/or monitored public spaces.

Photos and Videos

I already mentioned that your mobile device most likely geotags your photos and videos, which can tell you (or anyone else who has the files) where you were when the photos or videos were taken. Although that can sometimes be a privacy issue, a more common problem is controlling who gets to see your photos in the first place.

It's increasingly common for mobile camera apps to offer instant syncing of your photos to the cloud. That's tremendously convenient and useful, as it eliminates tedious manual steps, gives you an automatic backup, and makes sharing simpler. However, the fact that your images are stored in the cloud means that anyone with your username and password could potentially download all your photos and videos too. It has happened to celebrities, and it could happen to you, too. In fact, even without your credentials, there's always the possibility that a clever hacker could access your data somehow, or that your cloud hosting company suffers a security breach.

Of course, no one else *should* have your username and password. You can make it much more difficult for someone to guess it by choosing a long, strong, random password (I offer more detailed advice in *Take Control of Your Passwords*). You can also turn on two-factor authenti-

cation or two-step verification (see the sidebar About Two-Factor Authentication) if your cloud provider offers it.

Nevertheless, if you take photos or videos of an *intimate* nature—you know what I'm talking about here—it's not worth taking chances, and I suggest that you turn off all automatic photo syncing features.

iPhones and iPads can use iCloud Photos, which syncs all your photos from the Photos app. To stop using them, go to Settings > *your name* > iCloud > Photos and turn off Sync this iPhone (or iPad). But note that third-party photo apps may have their own syncing settings. For example, the Dropbox app can grab photos from your camera's photo library and upload them to Dropbox. So look through your apps for all such features and turn them off if you're concerned about keeping your photos private.

For other mobile platforms, the story varies from one device or app to the next. On an Android device, look in the settings for your photo-syncing app(s) (such as Amazon Photos or Google Photos).

Spear Phishing and Impersonation

Another broad category of attack you should be aware of—especially if you have an elevated risk level—involves savvy criminals who do their homework. Although these attacks are not exclusive to mobile devices, I mention them here because they're likely to involve your mobile device in some way, and they're certainly not restricted to email, web browsing, messaging, or other categories I discuss elsewhere.

In several other places in this book, I discuss phishing, in which someone tries to get you to reveal your personal credentials by taking you to a fake website or contacting you by phone or text. There's an even more sinister technique called *spear phishing*, in which someone gathers information about you (often from public sources, such as social media, or purchased from data brokers, say)—and then uses that information to persuade you, or someone else, to hand over more sensitive personal information (or money).

Unlike regular phishing, spear phishing is used to target a specific person—generally, someone with money, power, or influence—and it depends on gathering personal information about the target. Because the attacker knows some personal details about you, the likelihood that you'll go along with the scheme and give the attacker what they want increases.

The same techniques—gathering personal information about you from public or private sources—can be used to impersonate you or someone you know in other ways, too. For example, someone might email or text one of your family members, *spoofing* the From address or number so it looks like the message came from you. They could then claim that you're in trouble and need money, with instructions for sending the money to them directly. Or, they could claim to be from a government agency or bank, demanding money to settle some made-up claim based on real information about you or your property. The more details they know about you, the more persuasive their message could be.

Note: Using deepfake technology, an attacker could theoretically do the same thing with a call that appears to come from you—and even sounds and/or looks like you! At the moment, it's difficult and expensive to pull this off convincingly, but it's not at all impossible.

Sometimes impersonation attacks are indirect. Someone could call your cell carrier's customer service number, pretending to be you, tell a convincing story about a phone being lost or stolen, and convince the rep to assign your phone number to a different SIM card—one owned by the perpetrator. With control of incoming calls and texts, the attacker can then send "lost password" reset messages and receive the necessary codes via SMS or voice calls. In this way, they can gain access to bank accounts, email, and other private data.

Note: For a particularly harrowing recount of an attack that involved a SIM card swap as described above, read SIM swap horror story: I've lost decades of data and Google won't lift a finger by Matthew Miller at ZDNET.

Because spear phishing and impersonation attacks can be so sophisticated, guarding against them is challenging. Of course, using excellent passwords and two-factor authentication can both help, though you should avoid, if possible, two-step verification that uses SMS messages and instead opt for passkeys, authenticator codes, or hardware security keys. Making sure you've enabled a SIM lock on your phone is another helpful step. Ivan Drucker describes other approaches in Alternative Ways to Protect Yourself from Being Spearfished at TidBITS.

The best thing you can do to avoid impersonation attacks is to train friends, family, and anyone else who might unwittingly aid a spear phishing attacker to be suspicious. (You have to do this *before* any such attack occurs, of course!) If they receive a text, phone call, or email that seems to be from you but asks for something out of the ordinary, do one or more of the following:

- Ask them to contact you in a completely different way to confirm that it really is you they're communicating with. (A scammer will almost invariably make up an excuse as to why this is impossible.)
- Have them confirm a piece of information that only the two of you know. Nicknames and elements of inside jokes are often good choices.
- Can't think of something unique? Challenge them with a fake question. For example, "How is your dog doing after his surgery?" would elicit a confused reply from the real you if you don't have a dog, as would "Where is your cousin Steve living now?" if you don't have a cousin Steve. If the person on the other end of the conversation comes up with a quick reply ("Just fine, thanks" or "I haven't heard from him in a while") you know it's an impersonator.

Spyware

Here's a scary (and somewhat overstated) headline from a Wired story in May 2024: Apple's iPhone Spyware Problem Is Getting Worse. Here's What You Should Know. To summarize, some iPhones have been infected with malware that was installed remotely using what's

called a “zero-click attack”—the attacker takes advantage of one or more bugs in Apple’s software that lets them send a specially crafted iMessage that allows the spyware to infiltrate a phone without the user having to click anything or even look at a message. And, once the spyware is installed, it deletes the message it used to gain access to the phone, so the user could never even tell it happened.

According to that article, iPhone users in India were most likely to be targeted, but users in 150 countries around the world have been subject to such attacks. In all cases, however, these are specifically targeted attacks aimed at individuals such as journalists, political dissidents, and high-profile businesspeople.

On the one hand, if you are an ordinary person with ordinary privacy needs, you’re quite unlikely ever to encounter this type of spyware. And, Apple is certainly aware of the problem and taking steps to make iPhones less vulnerable to such attacks. On the other hand, you may have no way to tell for sure whether your phone is infected; the best indicator seems to be excessive battery drain for no apparent reason, although many other things besides spyware could cause that.

Apple says that Lockdown Mode should protect against spyware attacks; if you can’t use Lockdown Mode, disabling iMessage *should* make it impossible to be attacked in this way. The article also suggests restarting your phone at least once a day, because restarting the phone deletes the spyware (which would force the attacker to reinstall it). And, although that article is specifically about iPhones, there’s nothing to say Android phones might not have comparable weaknesses.

Last but not least, you should diligently keep your phone’s operating system up to date, because new versions routinely patch security problems like these.

Mobile Backups

Even if you disable cloud *syncing* of photos and videos from your mobile device, those images—along with your calendars, contacts, email, documents, and other data—may be *backed up* to the cloud. In

general, that's a good thing. I'm a huge proponent of backups, and for a mobile device, automatic, wireless backups to the cloud are by far the easiest way to get the job done. However, just as someone with your credentials (or someone who has hacked into a server) could download your synced photos, someone could download a backup of your data, restore it to a new device, and have full access to everything.

As with other aspects of mobile security, making sure your password is strong is an absolute necessity, and using two-factor authentication can only help. If the data on your phone is extremely sensitive, however, you might choose to forgo cloud backups and instead back up directly to your own computer.

If you have an iPhone or iPad, your best bet is to turn on Advanced Data Protection. For Android devices, turning off backups may be safer; see Back up or restore data on your Android device.

Privacy and International Travel

International borders pose significant challenges for travelers with electronic devices such as laptops and smartphones that may contain private data (in other words, pretty much everyone). When entering the United States, for example, customs agents are permitted to examine electronic devices for any reason or no reason. If your device is encrypted (as it should be!), the agents may ask for your password, and if you don't supply it (which you should not) they may impound your device for forensic examination, even if they have no grounds to prevent you from entering the country.

Appallingly, some travelers have also been asked for the passwords to their social media accounts at the border as a way of checking whether they're the "right" sort of person to enter the country. So, with or without access to the data on your devices, your *online* privacy may be at risk when you cross the border.

Whether or not such behavior is legal or justifiable, it happens—and you, as the traveler stuck in the customs line, have little recourse. Although I can't offer any solutions to this problem, I can mention some ways people have chosen to address this situation:

- If you use 1Password, enable Travel Mode to remove passwords from your devices before you reach the border.
- Encrypt the data on all devices and then *turn them off* before you get to the customs checkpoint; that way, they're less vulnerable to exploits that might examine their active RAM, and can't be unlocked with just a fingerprint or face scan. Decline requests for passwords, even if they mean giving up your devices temporarily.
- Securely erase all the data from your devices and then reinstall virgin operating systems before traveling. That way, a customs agent can examine an unlocked device, but there will be nothing to find. Data can later be restored from a backup or cloud storage.
- Use a "burner" phone and a cheap laptop when traveling, so that they can be erased or ditched without major consequences.

For further discussion of this problem, see A Guide to Getting Past Customs With Your Digital Privacy Intact at Wired, Can Border Agents Search Your Electronic Devices? It's Complicated. at the ACLU, or Getting Your Devices and Data Over the U.S. Border by Geoff Duncan (who edited this book) at TidBITS.

High-Risk Resources: Mobile Privacy

Your smartphone can pose a serious risk to your privacy; it can also be a lifeline in an emergency and an essential tool for dozens of day-to-day tasks. For most of us, ditching it altogether is not a reasonable option, though I suppose I would recommend just that if the stakes were high enough.

Short of such extreme measures, I would tell anyone facing a high risk of attack to do the following:

- On an iPhone, turn on Lockdown Mode; then enable Advanced Data Protection.
- Turn off your phone's location services completely.
- Turn off every setting on your phone that could be used to send your personal data to apps (as I discussed in Granting Apps Access Permission, Location Awareness, and Photos and Videos).
- Restart your phone at least once a day.
- On an Android phone, turn off Mobile Backups.

And, if you want even more protection, you could actually turn off your phone completely when you're not using it.

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 dyers. 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.

Smart Speakers

Smart speakers are voice-controlled devices that can play music, tell you the weather, control home automation equipment, tell you what's on your schedule, and more. Major players in this category include the Apple HomePod, Amazon Echo devices, Google Nest speakers, and Sonos speakers. I know people who have devices of this type in every room of their house, and they talk to Alexa or Siri or whatever as freely as they would any family member.

To state the obvious, smart speakers rely on microphones that constantly listen for keywords that tell them to take action, and rely on internet connections to process the commands you give and provide the music or information you ask for. So, by having a smart speaker in your house, you could be sending audio of literally everything that's spoken (or even just audible) in your house to some tech giant's servers. That, in turn, means there's an excellent chance that (with the notable exception of Apple HomePods) everything your speakers hear is used for ad targeting. (See, for example, What You Say to Google Assistant and Alexa (but Not Siri) Gets Used for Ad Targeting. Here's How. by Kaveh Waddell at Consumer Reports.) Maybe it's used for other things too. How would you ever know? And this is the sort of thing that a VPN or other privacy appliance would not change in the slightest way.

Is it just me, or does that seem super creepy? I'm pretty sure it's not just me.

Of course, the companies that make these products have impressive-sounding privacy policies. But, as you know, not every single employee and contractor and partner and partner-of-partners of every single tech company is completely trustworthy. Privacy policies are not always followed to the letter. And even if they were, bugs, hacks, and mistakes can always happen.

Is the convenience of being able to ask for your favorite music anywhere in your house worth the risk that everything anyone says in your house could be recorded, analyzed, and used for unknown reasons?

Look, it's your call, but if you say yes, don't bother inviting me to your house. If you can't live without a smart speaker, current evidence suggests that an Apple HomePod is *more likely* to keep your conversations private, but I still wouldn't discuss my plans for taking over the world in earshot of Siri.

Web-Connected Cameras

Let's turn our attention to a class of devices that you should definitely be quite anxious about: web-connected cameras. These come in every conceivable shape and size, with many different intended uses. There are, of course, doorbell cams. Other connected cameras are designed for monitoring your baby sleeping in the next room. Some (so-called *nannycams*) are for keeping an eye on the babysitter when you're out, and are often disguised or hidden in other objects. Many are intended as home security devices—they record all the activity in their field of view (often with motion activation) and can send it to the cloud or stream it to a mobile phone. Still others are built into toys and games.

Whatever the configuration or sales pitch, when you put a camera in (or outside) your house that's connected to the internet, *all the usual rules apply*. That is, you should assume that anyone on the internet can see everything the camera sees.

I know what you're thinking: I had to use a special app and go to a special site and use a special username and password! If I had to do all that, surely my cameras are safe from hackers. Right?

Yeah, not so much. One of the biggest reasons is that most people don't bother changing the factory-set default passwords for their security cameras, and those are easy to find. So easy, in fact, that a Russian website broadcasts live feeds of tens of thousands of cameras from hundreds of countries—all of them without their owners' knowledge, and many of them showing kids at play and other private household activity. (See Hacked Footage from Baby Monitors and Webcams Being Broadcast on Russian Site for one story about this site.)

So *of course* you should immediately change the password for any such device you use, and make it a good one. (Again, see *Take Control of Your Passwords* for advice.) But that may not be enough; devices such as these (or the servers they connect to) could have security flaws that give outsiders access. At the very least, I suggest turning off the cameras (or pointing them at a wall) when they're not in use, and as with streaming devices, read up on the manufacturers' security and privacy claims.

What About Tracking Devices?

Apple's AirTags and similar devices from other manufacturers use Bluetooth to track of the whereabouts of your luggage, bike, or pet. That can be very useful in cases where something is lost or stolen, but it goes without saying that those same tools can be used for nefarious reasons—say, to track your car without your knowledge.

Both Apple and Google have built mechanisms into their respective operating systems to make it easier to tell whether someone might be tracking you covertly (along with other privacy protections), but the systems are all imperfect. To learn more about the risks and how to mitigate them, see Glenn Fleishman's book *Take Control of Find My and AirTags*.

Other Connected Objects

When it comes to appliances, light bulbs, home-automation equipment, and the like, things get even more complicated.

Home security systems are designed to know when someone is at home, and in many cases, *where* in the home someone is—and that information could be misused in numerous ways. Perhaps your security company is completely trustworthy, but someone who hacks into your home system (or the monitoring company's computers) could learn enough to carry out a serious crime.

You may also be aware of the huge controversy that occurred back when Google bought smart thermostat manufacturer Nest. Since Google is in the business of learning everything about you in order to

sell advertising, users worried that their heating and cooling habits (and what those implied about their schedule, tastes, and so on) might be used for purposes they never agreed to. Google insisted that wouldn't happen, of course, and the controversy eventually faded. But then in February 2019, it came out that Nest Guard, a component of the Nest Secure home security and alarm system, contained a microphone that Google never informed its customers about. That was… troubling, to say the least.

It gets even worse. It's one thing if Netflix knows I binge-watched *Stranger Things* last weekend. It's another if some random company on the internet knows exactly when I'm away from home, asleep, or even in a particular room (because of the states of my home's smart light bulbs, thermostats, or whatnot). It's even more concerning to me if that data could be used to remotely unlock my door. That was the original idea behind Amazon Key, a system that (presumably due to public outcry) was changed so it can merely let people delivering packages for Amazon open your *garage* door and place the packages inside. Still…really?

And we're not done yet. Even *your car* is more likely than not to collect a worrying amount private data about you and send it straight to data brokers.

As I said earlier, even if the companies that develop these various internet-connected products are utterly trustworthy—and I obviously have some doubts about that—there could always be bugs or exploits that allow hackers to access them, and the range of potential problems is enormous.

Unfortunately, privacy controls for the average internet-connected Smart Thing are spotty at best—and with or without such controls, smart devices can be, and have been, hacked on a large scale (for example, to create a giant botnet to carry out a distributed denial of service, or DDoS, attack). Again, it doesn't matter much if the objects in your home connect to the internet via an encrypted router or a VPN; once the data is out there, someone could potentially find and use it.

Even more unfortunate, I can't offer any terrific advice here, except to repeat what I've said in other contexts: Be suspicious and circumspect when considering home automation products that involve microphones, cameras, sensors, or locks. Opt out of any nonessential data sharing. Don't use default passwords. And keep an eye out for software updates and other privacy alerts from the manufacturers that may enable you to nip security problems in the bud.

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

careful about sharing anything that has the potential to embarrass your child in the future.

As your child starts using online services without your supervision, you will undoubtedly want to teach them good privacy habits, and I hope the information in this book (especially in Take the Pledge) provides a useful starting point for discussion. If you instill a healthy sense of wariness from a young age, your child will be better equipped to fully take over the management of their own online privacy when the time comes.

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.

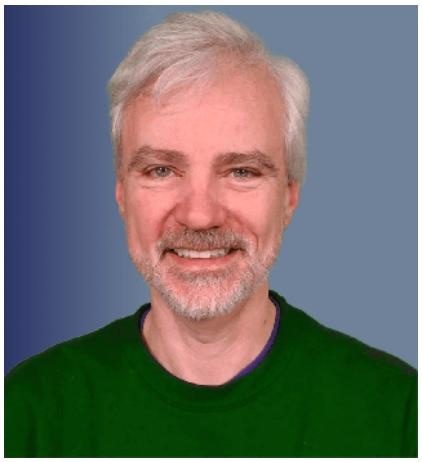
More Take Control Books

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.