TAKE CONTROL OF YOUR ONLINE PRIVACY

by JOE KISSELL

$14.99

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
Table of Contents

Read Me First .................................................................................................................. 5
  Updates and More ........................................................................................................... 5
  What’s New in the Fourth Edition .................................................................................. 6

Introduction ..................................................................................................................... 8

Online Privacy Quick Start ............................................................................................. 11

Learn What You Have to Hide ....................................................................................... 13
  Things You Might Want to Keep Private ........................................................................ 13
  Personally Identifiable Information ............................................................................. 16

Learn Who Wants Your Private Data (and Why) ......................................................... 18
  Advertisers .................................................................................................................... 18
  Data Brokers ............................................................................................................... 22
  Local Villains .............................................................................................................. 22
  Doxxers ....................................................................................................................... 23
  Hackers ......................................................................................................................... 24
  Big Media .................................................................................................................... 25
  Big Money .................................................................................................................... 25
  Big Data ....................................................................................................................... 26
  Big Brother ................................................................................................................ 26
  Foreign Governments ................................................................................................. 28

Understand the Evolving Online Privacy Landscape .................................................. 29
  The Curse of Free Stuff Continues .............................................................................. 30
  Major Data Breaches Are Increasingly Common ....................................................... 31
  Hardware Is Being Compromised ............................................................................... 31
  Big Data Is Harder to Get Away From ....................................................................... 32
  Privacy Laws Are Changing ....................................................................................... 34
  What About Privacy Policies? .................................................................................... 35
  Your Own Privacy Is Only Half (or Less) of the Problem ....................................... 37
  See How Bad Things Are ........................................................................................... 38

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
Develop a Privacy Strategy ........................................40
  Fix the Easy Things................................................40
  Create Privacy Rules for Yourself ..................................43
  Purge Your Info from Data Brokers..................................45
  Cope with Special Cases..............................................46
  Take the Pledge........................................................48

Keep Your Internet Connection Private .....................51
  Understand the Privacy Risks of Your Internet Connection ..51
  Prevent Snooping.....................................................55
  Turn Off Unnecessary Services....................................72
  Mind Your Camera and Microphone................................73
  Use a Firewall........................................................74
  Use an Outbound Firewall.........................................76

Browse the Web Privately ..........................................78
  Understand the Privacy Risks of Web Browsing ...............78
  Choose a Better Browser............................................82
  Go to the Right Site..................................................84
  Browse Securely.......................................................86
  Manage Local Storage of Private Data............................87
  Protect Passwords and Credit Card Info.........................99
  Search Privately........................................................101
  Browse Anonymously.................................................103
  Shop Online Privately...............................................106

Improve Email Privacy .............................................110
  Understand the Privacy Risks of Email .........................110
  Reduce Email Privacy Risks........................................113
  Encrypt Your Email..................................................125
  Send and Receive Email Anonymously............................130
  Use Email Alternatives.............................................130

Talk and Chat Privately ...........................................132
  Understand the Privacy Risks of Real-Time Communication ..133
  Improve Your Real-Time Communication Privacy ............135

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Social Media Sort of Private-ish</td>
<td>137</td>
</tr>
<tr>
<td>Understand the Privacy Risks of Social Media</td>
<td>137</td>
</tr>
<tr>
<td>Learn About the Facebook Problem</td>
<td>139</td>
</tr>
<tr>
<td>Check Your Privacy Settings</td>
<td>142</td>
</tr>
<tr>
<td>Use Other Social Media Precautions</td>
<td>143</td>
</tr>
<tr>
<td>Share Files Privately</td>
<td>147</td>
</tr>
<tr>
<td>Understand the Privacy Risks of File Sharing</td>
<td>147</td>
</tr>
<tr>
<td>Encrypt Transfers, Files, or Both</td>
<td>148</td>
</tr>
<tr>
<td>Use Peer-to-Peer File Sharing</td>
<td>152</td>
</tr>
<tr>
<td>Create a Personal Cloud</td>
<td>154</td>
</tr>
<tr>
<td>Manage Your Mobile Privacy</td>
<td>156</td>
</tr>
<tr>
<td>Cellular Data Considerations</td>
<td>157</td>
</tr>
<tr>
<td>Granting Apps Access Permission</td>
<td>160</td>
</tr>
<tr>
<td>Location Awareness</td>
<td>160</td>
</tr>
<tr>
<td>Photos and Videos</td>
<td>162</td>
</tr>
<tr>
<td>Mobile Backups</td>
<td>164</td>
</tr>
<tr>
<td>Keep the Internet of Things Private</td>
<td>166</td>
</tr>
<tr>
<td>Set-Top Devices</td>
<td>166</td>
</tr>
<tr>
<td>Web-Connected Cameras</td>
<td>167</td>
</tr>
<tr>
<td>Other Connected Objects</td>
<td>169</td>
</tr>
<tr>
<td>Maintain Privacy for Your Kids</td>
<td>171</td>
</tr>
<tr>
<td>About This Book</td>
<td>174</td>
</tr>
<tr>
<td>Ebook Extras</td>
<td>174</td>
</tr>
<tr>
<td>About the Author and Publisher</td>
<td>175</td>
</tr>
<tr>
<td>Credits</td>
<td>175</td>
</tr>
<tr>
<td>Also by Joe Kissell</td>
<td>176</td>
</tr>
<tr>
<td>Copyright and Fine Print</td>
<td>178</td>
</tr>
</tbody>
</table>
Welcome to *Take Control of Your Online Privacy, Fourth Edition*, version 4.0, published in April 2019 by alt concepts inc. 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 © 2019, alt concepts inc. 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.

- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our [Device Advice](#) page.)

- Read the ebook’s blog. You may find new tips or information, 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. However, if you bought this ebook elsewhere, you can add it to your account manually; see *Ebook Extras*. 

---

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
What’s New in the Fourth Edition

In the two years since the third edition of this book was released, it seems as though we’ve all been hearing about new privacy-related issues on an almost daily basis. Technology, legislation, and public opinion surrounding digital privacy are all undergoing rapid changes. As a result, this book required extensive modifications to bring it up to date. Among the most significant changes are the following:

- In the chapter Learn Who Wants Your Private Data (and Why), added a new entry: Foreign Governments

- Added a new chapter, Understand the Evolving Online Privacy Landscape, to provide the current lay of the land and point out areas that deserve more attention than they did previously

- Prefaced the topic Create Privacy Rules for Yourself with a new rule: be suspicious

- Updated Purge Your Info from Data Brokers with better and more current links

- Mentioned in a few places, including Use SSL If Possible, that usage of SSL on websites is rapidly on the rise—a very good thing

- Completely overhauled the topic Avoid DNS Mischief to cover the latest options in DNS providers and offer more detail on how to set them up

- Revised my advice in Avoid Malware to reflect what experts are currently suggesting for macOS and Windows users

- Greatly expanded the Mind Your Camera and Microphone discussion to explain why conventional wisdom about those two potential threats is not necessarily accurate

- Added the topic Choose a Better Browser to explore some of the best privacy-focused browser options

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
• Included numerous mentions of Apple’s privacy-related changes to Safari in Browse the Web Privately, especially in the sidebar Safari’s Evolving Privacy Features and Web Privacy Software

• Added Apple Pay and Google Pay to the list of ways to avoid letting credit card details get into the wrong hands in Shop Online Privately

• Updated the Improve Email Privacy chapter in two important ways: a new sidebar called Gmail Stops Scanning Email (yay!), a new topic Mind Your Incoming Email about spam, tracking beacons, phishing, and other threats, and a new sidebar Email Links: A Case Study

• Revised Talk and Chat Privately to remove mentions of defunct products and services, and add new ones

• In the Keep Social Media Sort of Private-ish chapter, added a big topic: Learn About the Facebook Problem; also gave additional privacy tips for Facebook

• Added Firefox Send to the list of options available to Encrypt Transfers, Files, or Both

• Updated the topic Other Connected Objects to talk about even more devices within the Internet of Things that could jeopardize your privacy

• Added numerous notes throughout the book pointing to recent news stories about privacy issues of various sorts

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
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 (or need) to. I like sharing thoughts and opinions with a wider audience online. 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 (or a family member) 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 I can make 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 often 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 whereabouts 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.

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, set-top box, cell phone, 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, 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 the United States, many 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.
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:**
- Think you have nothing to hide? Think again. Read Learn What You Have to Hide.
- Find out who might be trying to invade your privacy. See Learn Who Wants Your Private Data (and Why).
- Discover the (mostly negative, but occasionally positive) developments in the ever-changing world of online privacy in Understand the Evolving Online Privacy Landscape.

**Take preliminary steps:**
- Come up with a plan to deal with most common privacy issues in Develop a Privacy Strategy.
- Block the broadest and most likely privacy risks. See Keep Your Internet Connection Private.

**Use specific online services privately:**
- 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.
• Social may be another way to say “public,” but you need not give up all your privacy when using Facebook, Twitter, and other social networking services. See Keep Social Media Sort of Private-ish.

• Cloud backups and syncing could involve privacy risks if you’re not careful. See Keep File Syncing and Backups Private.

• There are many ways to share files online, but some of them may expose data you’d rather keep private. Read Share Files 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 set-top 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.
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. That’s what I want to help you understand in this brief chapter.

Bear in mind that 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. In the next chapter, 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 infor-
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 (see 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; this chapter shows 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

The web 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 that’s the only way most of them can make any money. However irritating or even slimy you may consider online advertising, it is the mechanism that has kept most websites and other internet services free.

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 thus lead to purchases. When advertisers make money, they’re able to keep buying ads and the sites that display the ads can stay in business.
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!), not those that are merely relevant to a site’s content or the perceived needs of a broad demographic group. 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.

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 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, the data stored locally on my device enables me to be identified 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 can build up 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.

Unless you regularly search for things that someone else might regard as suspicious, none of this should be a concern. After all, if I truly do want to buy an air conditioner, I’d rather see an ad for an air conditioner than an ad for weight-loss products or cars. Targeted ads should, in principle, be more helpful to me than random ads.
Understand the Evolving Online Privacy Landscape

Having acquainted you with what private data of yours may be at risk and to whom, 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.

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 even within the past year things have changed dramatically. You can’t treat privacy as a set-it-and-forget-it thing. You must remain informed and vigilant.

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

- Stronger privacy laws have come into effect; see Privacy Laws Are Changing, later in this chapter.

- More and more websites use SSL to encrypt connections by default; see Use SSL If Possible.

- Google stopped scanning Gmail to help it target ads (which I would have said is right up there with flying pigs and frost in the underworld in terms of likelihood, but it happened all the same); see Gmail Stops Scanning Email.

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

Although the web’s overall financial model looks approximately the same now as it did 20 years ago—from a distance, if you squint—the details are different. Now there’s much more “free” (that is, free-with-ads) stuff: not just content but also apps, data storage, online services, and much more. And we’re not paying for this stuff with only our attention (i.e., looking at ads). We’re paying for it with our privacy. So ruthless and greedy are the purveyors of online content that transparency, ethics, and legality are routinely ignored. For many of them, only ad dollars matter, and the less privacy you have, the more ad dollars they have. You can see where that leaves your private data.

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

But part of that is on us. We, the billions of people who use the internet every day, repeatedly and voluntarily give up our privacy—or other people’s privacy—to avoid paying for things. Whether our reward is greater convenience, no-cost tax preparation, or even a free pizza, 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.

And then there comes a moment of discomfort, when that deal turns into more than you were bargaining for. 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.
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 file sharing (all of which I cover later in the book).

I suggest dividing your privacy concerns into a few broad categories:

- First, **Fix the Easy Things**—that is, make simple changes to your software, settings, and habits that will address many of your privacy concerns but will require almost no planning or effort.

- 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.

- 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.

- Finally, **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.

---

**Fix the Easy Things**

You instinctively take measures to protect your real-world privacy—you draw the curtains at night, use a changing room to try on clothes, and lower your voice when discussing something sensitive in public. Adopting a comparable set of habits for online communication can
eliminate some of your most serious privacy risks. Better yet, you can make a number of simple, one-time adjustments to your devices and software that will improve your ongoing privacy without further effort.

I cover many of these “easy things” elsewhere in the book, but I’ll list some prominent examples now.

First, here are some one-time changes you might consider:

- **For your internet connection:** Follow the advice in Keep Your Internet Connection Private, including using WPA encryption on your Wi-Fi network (see Encrypt Your Wi-Fi Connection), turning on your computer’s firewall (see Use a Firewall), and fortifying your DNS settings (see Avoid DNS Mischief).

- **When browsing the web:** Use your browser’s built-in controls or third-party software to confirm that you’re not visiting fake or dangerous sites; see Go to the Right Site. Also, configure your web browsers not to store third-party cookies and other unnecessary private data, and consider blocking ads and trackers, too; see Manage Local Storage of Private Data.

- **For email:** Make sure your email program transmits your password in an encrypted form (see Log In Securely), or better yet, use SSL for incoming and outgoing mail (see Transfer Email Securely).

Next, consider adopting some new customs, such as:

- Always use a VPN to connect to the internet—at least when you’re on an open or unfamiliar network; see Use a VPN.

- Use a password manager to generate stronger passwords, store passwords and credit card data securely, and reduce the risk of phishing; see the sidebar Choosing Better Passwords, ahead, as well as Protect Passwords and Credit Card Info.

- Kick the Google (Bing, Yahoo, etc.) habit for searches; see Search Privately.

- If your device supports multiple user accounts, set up an account for each family member or coworker who uses it—with each account
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, set-top 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 far more secure, it has only recently begun to appear in consumer devices.

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 criminals. (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 domain names
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 or roommate might peek at the list of websites you’ve visited when you’re not looking. But some of this stored information, including cookies, is also available to advertisers and other online entities as you browse the web. One person may not care whether someone in his 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 (which I talk about ahead, in Browse Securely), 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
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 SSL to communicate with your email server.

- **On email servers:** The email server you connect to in order to send a message may hold onto that message only for as long as it takes to send it, and then delete it. Or it may cache the message for much longer—even indefinitely. Unless you run the email server yourself, you have no way to know for sure. (And trust me, you don’t want to run your own email server—I’m speaking from experience.) Once it reaches the recipient’s email server, it’ll stay there at least until the recipient reads it, but more likely it’ll stick around forever, because most modern email systems work best when the server stores the master copies of incoming messages, which then sync to client devices. In any case, for however long the message is on a server somewhere, anyone with access to that server could conceivably read the message without you or the recipient ever knowing.

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

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

I kid, but analog telephones are rapidly on the way out. My home phone, which I used to refer to as a “landline,” bypasses the phone company altogether and relies on a box that plugs into my broadband router. I happen to use Vonage for my home VoIP (voice-over-IP) telephone service, but I could have chosen a similar service from my broadband provider or from any of numerous other companies. In other words, for me, telephone service is a variety of internet service.

And then there’s my smartphone, which is almost never out of reach. I use it for conventional audio phone calls maybe once a week on average. Of course, I constantly use it for email, instant messages, SMS, Twitter, and video chats—most of which, again, travel over the internet—and even those occasional audio calls may use a VoIP app such as Skype.

Meanwhile, my computers and tablets have software for a long list of services that provide real-time text, audio, and/or video communication—not just Skype but also Google Hangouts, Apple’s FaceTime and Messages, and numerous others you may or may not have heard of, to say nothing of the chat services built into games, Facebook, and other social networking services. 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 attempt to 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 communica-
Keep Social Media Sort of Private-ish

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 Twitter, 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.)
Share Files Privately

In my world, “sharing files” generally means exchanging business documents such as word processing files, PDFs, and screenshots—maybe the odd font or disk image. I may be atypical in that regard. I have heard stories suggesting that people sometimes share less-wholesome files, including pirated movies, games, and software. If you’re tempted to do that, I invite you to skip back to Take the Pledge and follow the instructions there for avoiding online stupidity.

Having dispensed with that obligatory disclaimer, the fact is that what you have to share is none of my business or concern. You may have digital content of some kind that, for any of numerous legitimate reasons, you want to share online, but for which you have a privacy concern. In this chapter, I talk briefly about the privacy risks in file sharing and explore a few ways of addressing them.

**Note:** If you’re looking for the ultimate guide to sharing illegal stuff without getting caught, sorry—this isn’t it. I’ll outline the basics of private file sharing here, but remember: this book is about ordinary privacy for ordinary people.

---

**Understand the Privacy Risks of File Sharing**

To put it as concisely as I can, most privacy concerns with file sharing fall into one of the following categories:

- You want to share files with a specific person or group without letting anyone else know what you were sharing or with whom.

- You want to share files publicly, but without anyone knowing you were the person who uploaded or downloaded them.

Most methods of sharing files offer neither sort of privacy protection, which is why you may want to use extra precautions.
And what are the risks if you don’t? That all depends on what you’re sharing. Perhaps a competitor sneaks a look at trade secrets in confidential business files you’re sharing with your employees, clients, or contractors. Maybe the public gets early access to the top-secret new album, book, software, or game that you were only previewing for your agent or investors. Or the other side in a legal dispute sees potentially damaging information in a file you intended for your lawyer’s eyes alone. And, if you’re sharing copyrighted media, the copyright holder can rain all sorts of legal trouble on you.

### Encrypt Transfers, Files, or Both

A danger when sharing files is that their contents could be intercepted in transit between your computer and the recipient’s computer. You can reduce the risk of eavesdropping if you Encrypt Your Wi-Fi Connection or Use a VPN, but these measures protect data only for part of its journey. For end-to-end protection, the connection between your computer and the remote computer must be encrypted.

When you’re connecting to a file server, that generally means using protocols such as SFTP (SSH File Transfer Protocol), FTPS (FTP over SSL), FTP over SSH, or WebDAV HTTPS. Whatever you do, you should not use plain FTP (File Transfer Protocol), which is about the least secure file transfer method there is. (Not only is ordinary FTP not encrypted, but even your password is sent in the clear!)

However, protecting files while in transit may not always be an option—and even when it is, it only solves part of the problem. If a file is going to be sitting on a server someplace, and if you want to restrict access only to trusted parties, you might want to encrypt it as well—just as I suggested for sharing files by email (in Encrypt Your Email). This is true whether you upload to a public server or use any of numerous file sharing services such as Dropbox, Google Drive, SpiderOak One, or SugarSync.

Just before the fourth edition of this book was published, Mozilla (the organization behind the Firefox browser) launched a new, free service
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 increase your privacy in limited respects but put you at greater risk in other ways. I discuss these issues in Cellular Data Considerations.

- 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.

- 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.
Cellular Data Considerations

When your smartphone or tablet happens to be connected to a Wi-Fi network, the same rules apply as for any other device—barring the availability of WPA3 encryption, you should use a VPN to connect to the internet (see Prevent Snooping). But when you’re using your carrier’s cellular network (LTE, 4G, or whatever), you have to worry about some additional problems.

Your SIM Card

First, consider your device’s SIM card, which specifies its phone number, carrier preference, and so on. A report published in February 2015 revealed that Gemalto, the world’s largest SIM card supplier, had been hacked and its SIM card encryption keys stolen, with the result that security agencies in the United States and Britain might have the capability to decrypt any information—phone calls, text messages, or data—sent or received by any of countless millions of mobile users (see GCHQ and NSA Collaborate to Steal the Keys to Your Cellphone). The company conducted an investigation, and the resulting report makes the situation look considerably less dire than initially feared. In the worst case (if Gemalto’s claims are correct), attackers could have the capability to compromise 2G connections, but not 3G or later.

Nevertheless, I mention this story to point out that numerous factors influence your privacy—including things entirely out of your control like the security of the company that manufactured your phone’s SIM card. Assuming, however, that your SIM card’s encryption key was not in fact compromised, the content of most of your cellular communication is almost certainly much more secure than data transferred over an open Wi-Fi connection.

If you don’t think that’s a safe assumption, you can download apps that use their own encryption for voice calls—but the person on the other end of the conversation will need a compatible app too. I mentioned Silent Circle and Signal earlier; you can also use apps that provide their own encryption for text messages (such as Apple’s Messages when used with Apple ID accounts). And you can use a VPN on your mobile

Click here to buy the full 178-page “Take Control ofYour Online Privacy” for only $14.99!
Keep the Internet of Things Private

Computers, smartphones, and tablets aren’t the only devices that connect to the internet. My television, Apple TV, TiVo DVR, Blu-ray player, telephone, and home alarm system all have internet connections too. So do game consoles and music-streaming devices, not to mention many newer scanners, printers, cameras, and storage devices. So can 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.

Set-Top Devices

Let’s start with the first group—entertainment devices, typically those hooked up to your TV. (I know they no longer go on top of your TV, the geometry of flat-screen televisions being what it is, but they’re still commonly 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 will know 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 set-top box might infringe on your privacy:

- A set-top 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 limited—you may not be able to configure settings or install extra software as you can on a computer or mobile device, and using a VPN is generally out of the question. (Using a VPN Router can often help—it can provide a VPN connection to all your devices, albeit with a speed penalty. But assuming they don’t block you for using a VPN, video providers 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 set-top 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.

---

**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
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 preschool 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](https://www.coppa.org) (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 Twitter than on paper in an album. A few years from now, her classmates will be able to see it. All her future friends, love interests, employers, and children will be able to see it—so will unsavory characters you’d like to protect her from. And anyone who sees it will be able to share it with anyone else in the world. Is there any possibility your daughter might live to regret your choice?

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

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

• Never post anything online that could be used to predict your child’s location (including a route to or from school), at least when a parent isn’t around. This includes images with signs or landmarks in the background.

• No matter how cute your kid is in the bathtub, seriously, don’t post any nude photos online. (You did Take the Pledge, right?)

• Blog posts and other stories about your child’s behavior problems might have far-reaching consequences. Keep it positive.

• Kids say and do the darnedest things, but even though your children’s antics may entertain other adults, they could result in untold cruelty in the hands of a class bully a few years from now. Be super
About This Book

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

Ebook Extras

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

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

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

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.

- If you don’t have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control website, contact us.
About the Author and Publisher

Joe Kissell is the author of more than 60 books about technology. As of May 2017, he also became the publisher of Take Control Books, when alt concepts inc.—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 is also a contributing editor to TidBITS and a senior contributor to Macworld. 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 travel, walk, cook, eat, and practice t’ai chi. He and Morgen live in San Diego with their sons, Soren and Devin, and their cat, Zora. To contact Joe about this book, send him email and please include Take Control of Your Online Privacy in the subject. You can also follow him on Twitter (@joekissell) 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

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
Click any book title below to add more ebooks to your Take Control collection!

*Are Your Bits Flipped?*: Discover common tech misconceptions and how to avoid them.

*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 in macOS and iOS.

*Take Control of Backing Up Your Mac*: Protect your Mac’s valuable data from any sort of mishap.

*Take Control of iCloud*: Make the most of Apple’s online service for storing, syncing, and sharing data.

*Take Control of Maintaining Your Mac*: Learn preventive maintenance steps to keep your Mac running smoothly.

*Take Control of Speeding Up Your Mac*: Turn a slow Mac into a high-performance machine.

*Take Control of the Cloud*: Wrap your head around the wide variety of cloud services and apps, and make smart purchasing decisions.

*Take Control of the Mac Command Line with Terminal*: Master your Mac’s command-line interface and learn basic Unix skills.

*Take Control of Troubleshooting Your Mac*: Solve most everyday Mac problems without a trip to the Genius Bar.

*Take Control of Upgrading to Mojave*: Experience a trouble-free upgrade to the latest version of macOS with this comprehensive guide.

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

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
*Take Control of Your Paperless Office*: With your Mac, 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.

**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](http://example.com) as well as from venues such as Amazon and the Apple Books Store. But it’s a better user experience and our authors earn more when you buy directly from us. Just saying...

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

Click here to buy the full 178-page “Take Control of Your Online Privacy” for only $14.99!
Copyright and Fine Print

Take Control of Your Online Privacy, Fourth Edition
Copyright © 2019, alt concepts inc. All rights reserved.

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

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

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

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

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

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

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