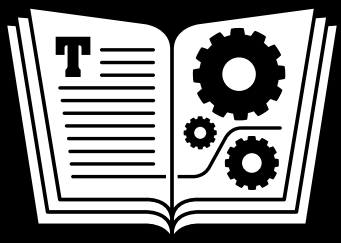
EBOOK EXTRAS: v3.0
Downloads, Updates, Feedback



TAKE CONTROL OF

YOUR ONLINE PRIVACY

by JOE KISSELL

$15

3RD EDITION

Table of Contents

Read Me First

Welcome to *Take Control of Your Online Privacy, Third Edition,* version 3.0, published in April 2017 by TidBITS Publishing 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. Also, you can Teach This Book.

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 Web site, 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.

Basics

If you're a Mac or iOS user and you'd like to review background information that might help you understand this book better, such as finding System Preferences and working with files in the Finder, read Tonya Engst's free *Read Me First: A Take Control Crash Course*, available on the Web or as a standalone ebook in PDF, EPUB, and the Kindle's Mobipocket format.

What's New in the Third Edition

Online privacy isn't getting any easier, and since the previous edition of this book, the world's governments, corporations, and criminals have been hard at work devising new ways to snoop on you. This edition updates the book in many ways, including the following:

- Added sidebars on numerous topics, including Privacy and Your ISP (ways your ISP may collect and sell your private data), Choosing Better Passwords (tips on password creation), About Two-Factor Authentication (why it's worth using extra authentication steps), Quantum Computing and Encryption (how computing advances could render all current encryption schemes useless), Beware VPN Review Sites (why such sites are often misleading), Using a VPN Router (protecting all your devices with a single VPN connection), Blur: The All-purpose Privacy Utility (a useful privacy app), and Privacy and International Travel (protecting your privacy when crossing international borders)
- Added further tips and advice in Purge Your Info from Data Brokers
- Greatly expanded the topic Use a VPN, with updated suggestions for choosing a provider
- Updated my recommendations for Web Privacy Software
- Added quite a few private messaging apps to Talk and Chat Privately, along with improved recommendations

- Revised and expanded my advice for encrypting files in Encrypt Transfers, Files, or Both
- Completely revamped Create a Personal Cloud to cover new personal cloud products
- Added a new topic about how to handle mobile apps that want access to personal data; see Granting Apps Access Permission

What Was New in the Second Edition

Version 2.0 of this book brought it up to date with the latest developments in online privacy as of early 2016 and added information on some particularly hot topics. The most significant changes were as follows:

- Added Data Brokers and Doxxers to the list of people who might want your private data
- Explained how to Purge Your Info from Data Brokers
- Included a sidebar, What about Adware?, that discusses this special flavor of malware designed to display intrusive advertising
- Added the topic Mind Your Camera and Microphone as another step to Keep Your Internet Connection Private
- Updated Web Privacy Software with more information on Adblock Plus and AdBlock; and provided additional recommendations in Search Privately, including a sidebar about Browsers with Enhanced Privacy
- Expanded the discussion of how to Encrypt Your Email with information on proprietary encrypted email services
- Added a new chapter, Manage Your Mobile Privacy, about additional privacy considerations when using a smartphone or tablet with a cellular Internet connection
- Added a new chapter, Keep the Internet of Things Private, on privacy for objects not normally considered computing devices

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. 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.

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:

- 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).

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.
- Share what you've learned about online privacy with your friends, family, or a large group. See Teach This Book.

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 Web site 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?

- **Purchases:** When you buy anything online, the vendor keeps a record. Your bank may know about all your transactions, too, including those made in person with a credit card. And 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 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 chats, instant messages, tweets, 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 Web site 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 can 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 Web sites 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 Web page 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 (see 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 (using a process called NAT, or Network Address Translation), and a device's address may change from time to time. When you visit a Web site, it records your 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 Web site 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. The basics:

- **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 harm you in your tent). Either way, you're anonymous from the bear's point of view (he 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 Web site 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 Web site, 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 (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 Web sites 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.

Web sites 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 Web sites 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 (which I discuss in Manage Local Storage of Private Data), but most involve using instructions hidden on a Web page that store data on my device when I visit one site (say, a search at Amazon.com) and then check that same data when I go to another site (say, weather.com) containing an ad from the same provider or advertising network. Although the server may store the details of my visit, the local data enables me to be identified across sites.

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 social networking site like Google+ 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.

But…

Individually targeted advertising isn't always to your benefit. The same bits of data 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. They could also

be used to determine that you are a registered voter in the "wrong" party, resulting in a phone call 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.

The variations on this theme are endless, but the point is that advertising can never be targeted with perfect precision. An advertiser may think it's 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.

When targeting becomes unfair or misleading, when it gives away personal information to others, or when it benefits only the advertiser and not the consumer, you may feel that your private data has been misused. Unfortunately, there's no master switch you can throw that says, "Sure, you can know who I am and what I search for, but only if you use that information responsibly." If advertising becomes intrusive or creepy rather than helpful, you may want to take steps to prevent any advertiser from collecting your private data, not just objectionable advertisers. As you'll see throughout this book, the number of ways in which you voluntarily give away personal data extends far beyond the Web sites you visit, so this isn't a problem with a perfect solution—but you can certainly reduce the risk.

Privacy and Your ISP

So far, I've 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, a more disturbing use of this data has recently been in the spotlight. Legislation passed in March 2017 by the United States Congress explicitly allows ISPs to sell browsing and usage data to marketers *without customers' consent or knowledge*, and in fact prevents the Federal Communications Commission from making rules that would disallow this behavior. The upshot is that there are now 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.)

The fact that ISPs are *allowed* to do this does not automatically mean they will. Some ISPs will undoubtedly refrain from selling customers' browsing data, possibly even using this privacy protection as a selling point over their competitors. Others may agree to protect your privacy in return for an additional fee. And some will, almost certainly, opt to make as much money as possible from your private data without the slightest remorse. I suggest checking your ISP's privacy policy and terms of service to see their current stance.

But all is not lost. Virtual private networks (VPNs) can often hide your browsing behavior from your ISP (see Use a VPN) and HTTPS and SSL connections (see Browse Securely) can prevent ISPs from accessing the content of your interactions with sites and services.

The Google Problem

Google isn't just a search engine; it's a provider of email, document storage, videos, phone service, and numerous other capabilities. What they all have in common is Google's legendary contextual advertising—that's how Google makes money. 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. Make no mistake about it: every search, every YouTube video viewed, every email read contributes to Google's personal profile on you, to be used for the express purpose of displaying targeted ads.

You can use other search engines and email providers, buy a non-Android cell phone, and watch videos on sites other than YouTube. But it's nearly impossible to avoid Google altogether (though some people try). By all 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 trust Google itself not to be evil with your data?

On one hand, it's not in Google's best interest to alienate its 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.

I won't say that you shouldn't trust Google. But 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.

And, even though I'm picking on Google here as the largest provider in its class, you shouldn't think other companies with comparable services (Microsoft, Yahoo, 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.

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 it can also be used to build up personal profiles (including people's interests, location information, habits, medical conditions, and anything else of interest) that 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:

- The Data Brokers: Selling your personal information at 60 Minutes
- Brokers use 'billions' of data points to profile Americans by Craig Timberg at the Washington Post

Local Villains

Another 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
- Neighbors with whom you have a dispute or disagreement
- 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
- Friends and relatives who like to snoop and gossip

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, Twitter, Flickr, 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, 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, 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 extremely long and growing fast.

Big Media

The RIAA (Recording Industry Association of America) and MPAA (Motion Picture Association of America)—along with record labels, movie studios, publishers, and other major copyright holders—are

keen to know who has been pirating their media. Apart from monitoring BitTorrent traffic and file sharing sites, these firms work closely with ISPs to identify people who illegally share movies, television shows, music, 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 file sharing 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 may be the largest non-governmental data collection entity in the world. But it's certainly not the only one. Facebook, Twitter, and other companies with users numbering in the hundreds of millions collect massive amounts of data on users' tastes, preferences, opinions, geographical whereabouts, and other details. Although this data is mostly used for targeting advertising (see Advertisers), 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).

Note: For a fascinating but also somewhat disturbing look at Big Data, see the online comic Terms of Service by Michael Keller and Josh Neufeld at Al Jazeera America.

Big Brother

Unless you've been protecting your privacy by living in a remote cave without electronics or human contact, you're probably aware of the string of revelations starting in mid-2013 about 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, 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 Global surveillance disclosures (2013–present) 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 the 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 U.S. government's current monitoring 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). Computers 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 use your information or for what purpose.

What about Privacy Policies?

Almost every Web site and Internet service has a published privacy policy, and I'd think twice about using a site without one. Privacy policies spell out what data the company collects (particularly personally identifiable information), 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.
- 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 it stores your data in a secret mountain fortress protected by a dragon, but does it have a contingency plan in case a hobbit shows up with a magic ring and a bunch of dwarves? These things happen.

- A privacy policy does not, by itself, have the force of law. If you can prove that a company violated its 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.

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 three 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, or take even stronger measures such as blocking all ads and trackers; 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 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 Web page 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, and if a connection uses WEP, an older security method, it's only a tiny bit more challenging. Newer Wi-Fi security protocols, such as WPA, offer protection that's much better—though still not foolproof (especially if the network's password is weak or can be guessed by brute force).

  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 what the other person said.

- **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.)

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 some 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 Web site 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 sneak a peak at the list of Web sites 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 his computer, but may have a principled objection to advertisers knowing about his 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 she's 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, information you send to, or receive from, a Web site 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, 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 impractical 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: The U.S. government currently needs a search warrant to access *unopened* email that's been stored online for 180 days or less—older unopened messages can be obtained with a (simpler) subpoena. But don't assume opened messages older than 180 days, or more-recent unopened messages, are off-limits; the law is 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 are more likely than not to 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, AIM (AOL Instant Messenger), 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 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

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.

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, tweets, LinkedIn updates, Instagram pictures, Yelp reviews, 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 paint a vivid and 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 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 Twitter that you're going on vacation (or just going to a concert), and burglars break into your house.
- 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.

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, 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.

One popular tool to encrypt files (while also compressing them) is WinZip—despite the name, it's available not only for Windows but also

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 and some tablets 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—unless you or your employer control the network and it uses WPA 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, 3G/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

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—consider Amazon Dash, devices that let you reorder specific products (like detergent) at the touch of a Wi-Fi–enabled button.

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. 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 his 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 Web sites 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

Teach This Book

This book helps you understand threats to your online privacy and take steps to reduce them. But what if you need to help other people make better online privacy choices? If you'd like to use the material in this book as the basis of a presentation, class, training program, or other teaching opportunity, we'd like to offer our assistance:

Share a Cheat Sheet

Lots of people won't read a book like this but still long for better online privacy. So we've developed a free, one-page PDF handout to cover the main points and key tips in this book. You can give it to anyone who needs quick advice. Download it here, and you can print copies for colleagues, send it to them via email, or share it online.

Order Classroom Copies

You can buy discounted copies of this book for classroom use. If you want to teach a group about online privacy, classroom copies are an inexpensive way to ensure that each participant has a copy of the book.

Download Training Materials

Not sure what to say in a course about online privacy? You can download a free, simplified presentation (in an iPhone- and iPad-friendly PDF format, with the option to buy an editable Keynote or PowerPoint file) that covers the main points in this book (contact us for purchasing details). Be sure to download the cheat sheet for your students too.

Hire the Author

For the ultimate experience, you can hire Joe Kissell to speak to your group about online privacy in person (or, if you prefer, by video). He's an entertaining and engaging speaker, and can work with groups of any size. Besides teaching the material in this book, he can customize a presentation to meet your organization's needs, answer participants' questions, and work with you to develop effective online privacy policies. For more information and a price quote, please contact Joe.

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 Web site, 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 Web site, contact us.

About the Author

Joe Kissell is the author of numerous books about technology, including *Take Control of Your Passwords*, *Take Control of Dropbox*, and *Take Control of the Cloud*. He is a contributing editor to TidBITS, a senior contributor to Macworld, and a popular speaker at conferences and other events.

When not writing or speaking, Joe likes to travel, walk, cook, eat, and practice t'ai chi. He lives in San Diego with his wife, Morgen Jahnke; 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.

Shameless Plug

To learn more about me personally, visit JoeKissell.com. You can also sign up for joeMail, my free, low-volume, no-spam mailing list, or follow me on Twitter (@joekissell).

About the Publisher

TidBITS Publishing Inc., publisher of the Take Control ebook series, was incorporated in 2007 by co-founders Adam and Tonya Engst. Adam and Tonya have been creating Apple-related content since they started the online newsletter TidBITS in 1990. In TidBITS, you can find the latest Apple news, plus read reviews, opinions, and more.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Geoff Duncan
- Production Assistant: Lauri Reinhardt
- Take Control logo: Geoff Allen of FUN is OK
- Cover design: Sam Schick of Neversink

More Take Control Books

This is but one of many Take Control titles! Most of our books focus on the Mac and macOS, but we also publish titles that cover iOS, along with general technology topics. You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the iBooks Store. Our ebooks are available in three formats: PDF, EPUB, and the Kindle's Mobipocket. All are DRM-free.

Copyright and Fine Print

Take Control of Your Online Privacy, Third Edition
ISBN: 978-1-61542-485-6

TidBITS Publishing Inc. 50 Hickory Road Ithaca, NY 14850 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, he or she 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 TidBITS Publishing 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 TidBITS Publishing 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.