"We all need to protect our digital privacy.
This book provides real-world examples and the guidance
we need to protect ourselves and our loved ones."

JOHN LEE DUMAS

PRIVACY CRISIS

How to maintain your privacy without becoming a hermit

CHRIS PARKER

Published by Screaming Bunny in Tustin,

California on October 1, 2025.

www.privacycrisis.com

ISBNs
Trade paperback: 9798992521900
Hardcover: 9798992521917
Audiobook: 9798992521924
Kindle: 9798992521931

Contents

Dedication

I dedicate this book to you, the reader:

In a world where your data is currency, your choices matter. This book is for those who refuse to be complacent, who ask questions, and who demand the right to privacy.

May this book empower you to take control, make informed decisions, and safeguard what is rightfully yours.

-Chris Parker

Introduction

Personal information rarely seems valuable to anyone who doesn't have a comprehensive education in information security – indeed, we often eagerly give it away for free to social media companies and anyone who will listen to us at a cocktail party – but even our most mundane details can be extremely valuable to corporations and thieves. If someone knows who you are, then they can find out what you own and what you want, and they can use that information to get what *they* want from you. Fortunately for all of us, very few people are willing and able to be that greedy and manipulative, but sociopaths and corporations aren't so burdened by empathy and morality.

Once your personal and/or private information has been collected by a third-party, it immediately becomes a force that works against your interests. Online data collectors seek to know as much about everyone as possible so that they can direct each person toward a sale, signup, or piece of propaganda – not just on the Internet, but in the offline world as well. That's bad enough, but even worse is the fact that you don't know what will happen to your personal information after it's been collected. Data brokers, advertising platforms, and social media companies often sell or share their data hoard to or with other companies without your knowledge or permission.

Given its value, you'd figure that data collectors would spare no expense to protect the information they've harvested, but in reality they are often extremely careless; every few hours, scammers and thieves steal millions of records of personal data from a company or local government office[1], and you might not be notified if you're one of the victims. Some of the targets are companies you've never heard of, but the largest and most damaging data breaches have consistently been well-known corporations; X / Twitter, for instance, made the top ten list of worst data breaches in 2022… *twice.*

So why does this matter, and what can you do about it?

Before I answer those questions (and I *do* answer those questions in great detail in this book), I feel it's important to help you put the negative aspects of privacy and information security into perspective, and give you the emotional and social tools to understand what's possible without losing confidence in your ability to handle it. My position is that I don't need to scare the crap out of you to get you to buy this book – that would be hypocritical of me, in fact – so I really want you to read the "Privacy Without Paranoia" section later in this Introduction. Don't skip ahead!

I also don't want to leave you hanging, so before I tell you about all the bad things that can happen, I'll equip you with the tools and skills to prevent or mitigate them. In Chapter 1 I cover a few critical actions you can take immediately to increase your personal safety, financial security, and privacy. In Chapter 2 I explain some extra measures that aren't as urgent, but are no less important. You definitely should not skip any section in Chapter 1, though I feel it's reasonable to skim through Chapter 2 and come back to it later if you don't have the time to do everything in it right now. Don't forget to come back to it, though.

What exactly do I mean when I refer to *personal information* and *private information?* And what's the difference between *information* and *data?* Are some kinds of personal information more dangerous than others? In Chapter 3 I define these terms, and establish a standard three-level paradigm for categorizing personal information: public, private, and secret.

Data collectors operate both legally and illegally, and can obtain valuable information from a wide variety of sources. In Chapter 3 I tell you who

---

[1] *https://www.pcmag.com/news/cybercrime-in-2022-fewer-data-breaches-but-more-victims*

they are, what they might know about you, what they typically want, and how they record and collect your information. I also take a close look at the methods thieves typically use to steal personal data from ordinary people, small businesses, and large corporations.

In Chapter 4 I explain in depth – with real world case-study examples – how you can be harmed directly when thieves, scammers, unethically-managed corporations, and Internet vigilantes and "social justice warriors" have access to your personal information. Where *Privacy Crisis* stands apart from most books on information security and privacy, though, is on the much broader topic of **indirect harm** resulting from a data breach or overexposure to highly-targeted marking campaigns, which I cover in Chapter 5: overspending; psychological self-harm; development of addictions and compulsive behaviors; and violence, civil unrest, and various self-destructive behaviors inspired by disinformation, misinformation, and propaganda.

If you follow my guidance in the first two chapters of this book, then you'll be reasonably well protected against identity theft and the worst forms of corporate marketing. It's a certainty that at least some of your personal data has already been collected, sold, and stolen several times, though. Chapter 6 contains instructions and advice for getting off of mailing lists, blocking hidden digital trackers, and learning how to protect yourself from the influence of disinformation and propaganda.

Most people surrender their personal information to data collectors as a matter of convenience. By embracing privacy and information security, you are protecting yourself and your family from various harms, but this is not without cost. In Chapter 7 you'll learn how companies subtly punish people for dodging their data collection and marketing efforts. Is it worth trading your dignity and agency for conveniences and discounts?

We often make our personal details available because we want certain people to be able to easily find us – clients, customers, job recruiters, and long-lost friends. You can protect your personal information without being a recluse. In chapter 8, I explain how to be found without substantially increasing your risks.

By the time you reach Chapter 9, you'll have increased your privacy by understanding how and when your personal data is collected, and you'll have taken steps to ensure that anything the data collectors and Internet

thieves already have is of minimal value to them. So what's next? In Chapter 9 I show you many ways that you can make the world a better place by selectively allowing "good" information collection in certain circumstances, helping others (especially the vulnerable) to maintain their privacy, and supporting politicians and businesses that honor privacy as a fundamental component of freedom. If enough people make the right choices in elections and with their purchases, we can create a future where online scammers, spammers, identity thieves, and influence marketers are obsolete.

Finally, I offer a preview of what an institutionally pro-privacy future might look like. All levels of government in the Western world are marching – at various speeds – toward reducing the amount of personal data that can be legally collected, how it can be stored and secured, and with whom it can be shared. Unfortunately there will always be scams that seek to circumvent or work around security measures and safeguards. In an environment that is hostile to data collection, advertising, and identity theft, how might thieves and marketers of the future try to get through to us?

Privacy Without Paranoia

When it comes to protecting your privacy and personal information, there is just as much (perhaps more) danger in going too far as there is in not going far enough. The biggest challenge for me in writing and marketing this book was to accurately explain real privacy and security risks – and how to reduce or avoid them – without inspiring or amplifying paranoia in my readers.

Fear is a powerful motivator and an effective (if immoral) sales tactic, but indulging in it never benefits the believer. The more you think about protecting yourself against imagined threats, the less able you are to defend yourself against actual danger. Paranoia forces you to become disconnected from the real and rational world; it causes you to feel isolated, and isolation leads to more paranoia. Worrying about things doesn't make them less likely to happen, and in most cases it doesn't help you prepare for or avoid whatever you're worried about – in fact, paranoia makes you *more* vulnerable because it erases the boundary between real and imaginary threats; it erodes trust and rational thinking, which makes it difficult for people to separate credible threats from made-up ones. Eventually the

paranoid person is no longer able to distinguish between fact and fiction, and has no credible resources to consult because he or she has learned to distrust "the mainstream media," rational-thinking friends, and skeptical relatives. Late-stage paranoia pushes people to trust only the information sources that validate and reinforce their irrational fears, even if they're full of lies and propaganda.

In the Information Age, paranoia is a big business. Demagogues, corporations, and national governments are constantly trying to influence our thoughts, decisions, and actions in service to their goals, *always* at your expense. Conspiracy theory peddlers have made a fortune from fomenting and stoking unreasonable fears in their followers. The actions they inspire people to take are rarely effective, usually involve spending money in their online store or on their sponsors' websites, and are often counter-productive or self-destructive.

In writing this book, my intention is to provide you with actionable knowledge and credible skills that will enable you to protect yourself from *real-world* threats and concerns, and to quickly and effectively handle identity theft (or other information-related crimes) if it happens to you or someone you know. I have also made an effort to teach you how to identify and disregard imaginary or exaggerated dangers, but if you've already invested in the false realities and scaremongering of con-artists and disinformation peddlers out there, then there isn't much I can do to counter their propaganda except to say this: Stay calm and be skeptical. If someone is trying to make you feel an emotion and inspire a sense of urgency, then they are attempting to manipulate you. Here's the same thing expressed as a formula:

```
Emotion + Urgency = Manipulation
```

The key to preventing yourself from succumbing to paranoid thinking is **mindfulness**. Be mindful not only of how you feel, but of what you're imagining. If you find yourself catastrophizing about what will happen to you if you don't take ownership and control of your personal data immediately, or if your thoughts often begin with "What will happen if…" or "But what will I do when…" then you're on the path to paranoia.

You don't need to prepare for every possible *situation;* you only need to be prepared to handle *situations* in general. You don't need to plan and perform a separate fire drill for every room in every building before you

enter it; you only need to know the basic guidelines and rules for safely escaping burning buildings. The unfortunate reality is that you can still be trapped in a burning building no matter how knowledgeable and practiced you are (a fact which is illustrated to comedic extreme by Ben Stiller's character in the Wes Anderson movie *The Royal Tenenbaums).* You cannot control the conditions that led to that situation; all you can control is how you handle it. Therefore *training* is generally good, but *preparation* usually is not because you cannot know the exact conditions of any future situation. I don't want you to follow a script; I want to teach you how to improvise.

Some people enjoy learning new things and expanding their view of the world, and other people learn something new and become so terrified that they sabotage themselves trying to avoid potential but unlikely consequences. Avoidance is often a bigger problem than whatever you're trying to avoid because while the catastrophe you're imagining may never happen (and most imagined catastrophes will *never* happen), the sacrifices required to avoid it are instant and perpetual. It isn't reasonable to be so afraid of being trapped in a burning building that you avoid buildings altogether.

The subsections below illustrate these points in greater detail.

Risk is Relative

One of the best ways to sabotage yourself is to spend too much effort worrying about low-probability threats. This is not to say that low-probability dangers aren't worth considering or attempting to mitigate or prevent, but the resources you spend on this should be commensurate with the probability of its occurrence, not the level of fear it inspires.

Let's put the odds into perspective. While any form of cancer is frightening, it might seem that lung cancer in particular isn't much to worry about if you've never smoked cigarettes, haven't been exposed to asbestos, and don't work in a coal mine. There's still a substantial risk even without those factors, though. For US citizens, the odds of getting lung cancer at some point in life are approximately 1 in 16. What would you pay to reduce your chances of getting lung cancer by 11%? How about $200? Most radon

gas detectors are less than $200, and prolonged radon gas exposure in the home or workplace is the second leading cause of lung cancer in the US[2].

Similarly, only a few hundred people per year die of carbon monoxide poisoning in the US. In most circumstances, the odds of dying from CO poisoning are tiny, but the cost of preventing those deaths is so low that the fact they occur at all is truly tragic: $50 or less for a carbon monoxide detector. In fact, your $200 radon detector probably also functions as a carbon monoxide and smoke detector.

You cannot control what other people do; you only have control over your own decisions and actions. You can be a perfect defensive driver, and someone who is drunk or distracted can slam into your car, destroying your vehicle and causing you injury. We all face these risks – and more – every time we sit in the driver's seat, so we do what we can to mitigate the damage: wear a seat belt, keep the car well-maintained, obey traffic laws, drive defensively, and retain an appropriate level of insurance coverage. If you're feeling anxious, try to find peace of mind in the assurance that you've done everything you can do to ensure your safety without avoiding driving.

Don't Panic

I'm going to tell you what the potential consequences are of ignoring your data rights, but the risks and likelihoods can vary. Just as with random tragedies, the worst things rarely happen, and even when you're careful you can still get hurt. There are many things you can do to mitigate risks and damage. Don't ask if it's possible – an attack is *always* possible – ask how much effort and resources it would take to successfully pull it off, and what the payoff would be for the attacker. For instance it isn't reasonable for a thief to spend $15,000 on tools and information to break into a bank account that only has $50 in it; a car that is not worth stealing isn't worth the risk of getting caught stealing it; your spiral notebook full of billion-dollar business ideas or blockbuster movie plots is not nearly as valuable as you think it is – *no one* is going to steal it (except, perhaps, as a prank). Crimes of opportunity do happen on rare occasions – objectively worthless

[2] *https://www.lung.org/lung-health-diseases/lung-disease-lookup/lung-cancer/basics/what-causes-lung-cancer*

things may be stolen without much prior consideration of their street value – but that's not the sort of thing I'm talking about here.

There are rare circumstances in which higher security will potentially yield a greater loss. For instance if you don't keep anything of value in your car, then it may be more cost-effective to keep the doors unlocked. Thieves expect to need to break into a car to steal something from it, but it's worth their time to see if the doors are unlocked first. If a thief smashes the window or punches the lock, it will cost you hundreds of dollars to repair the damage. If you left the doors unlocked, the thief might just open a door, find nothing of value, close the door, and move on to the next car. If, however, you do keep valuable things in your car, locking the door probably won't prevent them from being stolen if they can be seen through the windows, or if a thief has observed you putting something valuable in the trunk.

Skepticism and Truth

The most important tool in your data rights box is **skepticism**. Not only will it help prevent your personal and private data from being used against you, it will also prevent bad information from entering your consciousness. It may seem like *protecting your data from being collected,* and *refusing to believe false narratives* are unrelated concepts, but they are not; for someone to become a willing participant in a process or scheme that will victimize them, they must first accept one or more false narratives in the form of lies, illusions, marketing slogans, political propaganda, or a dishonest assurance of trust and safety.

Truth and **trust** are the foundation of good mental hygiene; skepticism is how we preserve and protect that foundation. Those who refuse to be skeptical whenever they're asked to give out their information, or when they are asked to believe and act upon new information about people and events, are primed to become victims of scams, cults, disinformation peddlers, online harassment, stalking, and corporate marketing campaigns. In the most extreme cases, sharing or believing the wrong thing can lead you into physical harm or jail time.

Whether you're being asked to share your date of birth with a stranger over the phone, or being asked by a friend to watch a video that promotes a conspiracy theory, you are best served by training yourself to react immediately with skepticism, even if the source was previously trusted.

Always question the authenticity of the source and the necessity of participating in whatever you're being asked to do. When you're asked to share your personal information, here are some good questions to consider:

Why is this information necessary?

In most circumstances you don't have to play by other people's rules. Just because someone asks you for personal or private information doesn't mean you *must* provide it. Even if it's a "required field" in an app or an online form, you aren't usually required by law to provide complete or accurate information.

Obviously if you're ordering something from an online store, you must provide a shipping address, billing address, and payment information. It will probably benefit you to provide your phone number or email address as well, in case there are problems with the order. Unfortunately this is likely to get you onto email and direct mailing lists, even if you did not opt-in to them. While financial institutions and the local and federal government require you to truthfully and accurately provide a physical home address when requested, you're free to have all other mail and deliveries sent to a post office box or mailbox service. (This is covered in more detail in Chapters 2 and 6).

Never provide more information than is absolutely necessary. Your dentist, for instance, does not need your social security number or a photocopy of your driver's license. If you ask why he or she needs this information, likely you'll be told a false narrative in order to coerce you into participating; most commonly it's ostensibly for "identification" or "security" purposes. There are better ways to identify you that aren't inherently risky. Besides, how does the dentist know that you aren't using someone else's driver's license and SSN? And what happens if someone doesn't have a driver's license – does the dentist refuse to treat them?

Internet and cellular service providers also often ask for part or all of your social security number for "identification" or "security" purposes. The last four digits of a social security number are very commonly used as a kind of password or PIN. That being the case, the companies collecting this information have no legal method of validating it, so you have absolutely no reason to provide the correct number – just make sure you remember

the fake one, or record it securely (I provide guidance and instructions for this in the "Use Dummy Information" section of Chapter 2).

The only scenarios where you need to provide your social security number to a commercial entity are: to receive Social Security benefits, and to perform a credit check. Most commonly it's for a credit check, which you must explicitly agree to because this inquiry will be recorded by credit agencies. In some cases a credit check is not strictly required, but without it you may have to pay a deposit to establish service.

Even if you think some piece of information is harmless – or even if you know it's already public, or at very least not secret – don't reveal it if you don't absolutely have to. Many companies require people to provide answers to "security questions" to validate their identity or account ownership. As I explain in Chapters 1 and 2, this is a very poor method of securing an account because the answers are rarely secret.

How will this information be stored, and when will the records be destroyed?

If any of your personal or private information is written on a piece of paper, where will that paper be stored, who will have access to it, and when and how will it be disposed of? If the person you're talking to can't easily answer these questions, then don't trust them with any non-public information.

Even if you trust your dentist, you don't know who else will have access to your dental, health, financial, and other data that he or she collects. A disgruntled employee or criminally-inclined janitor can easily open a filing cabinet and steal paper records, which may give them enough information to harm you financially or socially.

All paper records must be shredded (cross-shredding is best) when they are no longer necessary. All digital records must be encrypted in transit and "at rest" (meaning the hard disk drive it's stored on is encrypted; there's more information on this in Chapter 1). Assume that any non-encrypted data will become public at some point.

With whom will this information be shared?

Companies sell customer data to other companies all the time. It's no secret – in fact the company will tell you about it in its "privacy policy!" Some jurisdictions require companies to offer a method of opting-out of information sharing; if possible, do it. At the very least it's good to know which other companies will be using your data, but sometimes even that isn't possible. For instance, Google will share the information it collects about you with its advertisers, which encompasses every person and company that uses the Google Ads service.

Is this how this person or company usually contacts me?

Never give out any personal information to someone who initiates contact with you. If you are required to reveal your data to a person or company, you must initiate contact with them through official channels (the phone number or email address published on the official website, or printed on the back of your debit or credit card). For instance if you get a phone call from someone claiming to be from your bank, and the first question they ask is for your account number or social security number, hang up. Next, obtain the bank's official phone number from a trusted source such as the official website, the back of your debit card, or from a known-valid statement or other official written communication. Be skeptical of any written communication that seems even slightly suspicious; it is very easy to fabricate an invoice, bill, or bank statement.

There's a popular telephone scam involving a robo-call claiming to be from the US Internal Revenue Service. The only reason this scam works is: victims aren't aware that the IRS will never request payment or other personal information over the phone[3] (other than perhaps a mailing address, if their previous attempts to contact you by US mail were not successful). While you can call or email the IRS yourself, all critical IRS-initiated communication (and all requests for payment) is strictly limited to paper mail.

[3] *https://www.irs.gov/newsroom/understanding-how-the-irs-contacts-taxpayers-avoiding-scams-and-how-to-know-its-really-the-irs-reaching-out*

If your bank or brokerage has never called you by phone in the past, be skeptical!

Is this person calling / texting / emailing / mailing from the official phone number, Web domain, or mailing address of the company they're claiming to represent?

If you get an email claiming that you owe money to a certain company, then the email address it's coming from should be using the company's official domain. For instance, Best Buy will never send you a bill or invoice from a Gmail or Yahoo Mail address.

All legitimate business phone calls should originate from either a toll-free number (800 or 888), or the area code where the company is based. Even if the number is legitimate, don't give out any information to the caller unless you initiated contact; skilled scammers know how to spoof caller ID phone numbers.

Is this message designed to inspire an emotion, and does it have a sense of urgency?

Many people learned to distrust strangers from the now-disfavored "stranger danger" rhetoric in childhood. The reason why this philosophy has fallen out of favor is the fact that 90% of all instances of childhood sexual abuse are committed by people the child knows and trusts[4]. Therefore, not only is "stranger danger" ineffective in preventing sexual abuse and abductions, it also helps conceal the true perpetrators.

But what about the 10% of sexual predators who actually *are* strangers? Child Safety Educator and author Pattie Fitzgerald (safelyeverafter.com) offers a much more effective philosophy for parents to teach their children: beware "tricky people," whom she defines as "anyone who gives you that 'uh-oh' feeling." Sexual predators seek access to, and privacy with, their targets. To achieve this, they often offer gifts such as toys or candy, or ask kids for help with something – directions to someplace, finding a lost pet, carrying a package, etc. Safe adults only ask for help from other

[4] *https://www.cdc.gov/child-abuse-neglect/about/about-child-sexual-abuse.html*

adults, not children, and when they do legitimately want to give a gift or enlist a child to help with something, they'll get permission from the kid's parents first.

This advice conveys perfectly into adulthood, though the tactics that predators use on adults are much more complex. Obvious scams tend to be ineffective, so scammers try to obscure their true intentions by using a false narrative to create an emotional reaction. Our emotions can easily override our rational minds. Sometimes this is in the form of joy – telling you that you've won a lottery or contest – and sometimes anger or fear, but regardless of which emotions they're targeting, every false narrative creates a sense of urgency. This can be direct, such as a caller telling you that you need to wire money to get your daughter out of jail; or it can be indirect, such as emailing you a phony invoice from a service that you would never use. As I write this, two of the most popular email invoice scams involve annual subscriptions to Best Buy's "Geek Squad" or Norton Anti-Virus. Usually they claim to have already charged your credit card, which is something you can easily verify on your own through your bank or credit card company. Again: when in doubt, go directly to the company's official website (don't click the link in the PDF or the email) and call the official phone number yourself.

Basically if you *feel* like you're being tricked, coerced, or manipulated, then you are.

How could a thief or stalker benefit from this information?

Nearly any fact about you can be used to create a credible false narrative. Let's say, for instance, that you're a Taylor Swift fan. Millions of people can make the same claim; not only is this not a secret, it's also not even remotely unique. But if a scammer knew your name, phone number, the city you live in, and the fact that you're a Taylor Swift fan, he or she could call you, claim to be a Ticketmaster sales representative, and offer you two floor-level tickets to her as-yet unannounced concert next month at a venue in your city. They're only $150 each, but you have to buy two and you have to buy them right now over the phone!

With a healthy sense of skepticism, this false narrative crumbles fairly easily.

A thief doesn't need to know very much information about you in order to craft a false narrative that you're likely to identify with. Likewise if a stalker – an ex-lover, let's say – knows where you work, he or she can disrupt your career by calling the office or by skulking in the parking lot.

Unfortunately if you've ever had a social media account and "liked" or "followed" official pages or groups for the celebrities, art, and hobbies you enjoy, then that information's already out there and you're unlikely to be able to completely erase it. From now on, though, be conscious of what you "like" or "follow," and take a moment to think about what kinds of facts about you are likely to be public so that the next time you're confronted with a false narrative, your skepticism will be more accessible.

The Cost of Lost Trust

As human beings we are social animals; we have evolved to thrive in communities among people we know and trust. Unfortunately modern society has outpaced our natural evolution, and we now live in a world composed of many overlapping communities of various sizes and degrees of familiarity. The people around us at any given time are not necessarily members of our communities anymore; even if they are, we don't always know them well enough to trust them with our safety and well-being.

Trust is our most valuable asset and our biggest weakness. Without trust we cannot function in society, nor can society function without at least a minimum amount of it; this is why our laws are designed to protect our sense of trust above all else, and why the worst non-criminal social transgressions are rooted in betrayal. It's useful to think of trust not as a binary yes-or-no concept, but as something that exists in degrees. For instance you might trust your college roommate not to steal your wallet, while simultaneously *not* trusting him not to steal your frozen pizza. Regardless of the financial value of these two items, the moral transgression of stealing one's wallet is not nearly the same as of stealing one's pizza. That's not to say that value isn't a factor; you may also trust your roommate not to steal $20 from your desk, but would be wary of letting him know that you're hiding $20,000 under your mattress. That's probably an acceptable level of trust for a roommate. If you didn't trust him at all, then it wouldn't be possible to be roommates with him.

It is not the circumvention of our trust by grand betrayals or complex heists that we're most often sabotaged by, though. Rather, it's the implicit

trust we give to people, businesses, and places that we recognize and are familiar with. We're all naturally wary of strangers (especially if they seem very different from us), but they're not usually our enemies. According to the US Department of Justice[5], your friends, acquaintances, and loved-ones in collective – the people you trust, to some degree – are about 4% more likely to commit a violent crime against you than a complete stranger. When in doubt, ask yourself if the person you're dealing with could profit more from a betrayal than an honest deal. If someone will derive the most benefit by legitimately building trust with you, then you can be about 90% sure that your interactions with them will be safe and honest. That last 10% is reserved for taking extra measures to ensure that your assumptions are true.

Without trust, civilization doesn't work; on the other hand, without trust, scams don't work. If you're having trouble figuring out where to draw the line, think of it this way: trust is always an *act* of faith, but it should never be a *leap* of faith. When the stakes are legitimately high and you're unsure of your level of trust, consider former US President Ronald Reagan's philosophy on working with the leaders of the Soviet Union: "Trust, but verify."

We don't need to verify most things, though, especially if they are unlikely to be false, or if there is no consequence in accepting them anyway. To function normally in society, we must accept certain low-level assumptions so that we can be productive, cooperative, and peaceful. For instance you don't need to verify that every $1 and $5 bill you receive from a bank teller, ATM, or retail cashier is real. At a glance it looks and feels legitimate, so you assume that it is. Bill denominations of $20, $50, and $100 deserve more scrutiny because they are vulnerable to counterfeiting. The materials and equipment required to create a high-quality counterfeit $1, $5, or $10 bill are higher than the face value; thus, you can safely assume that every one of them that you receive from a reasonably trustworthy source is legitimate, and you don't have to test them. Likewise, we do not need to independently investigate every email, text, link, social media post, and article we read, so long as they aren't a surprise, the stakes are low, and there isn't anything suspicious about them.

---

[5] *https://www.ojp.gov/ncjrs/virtual-library/abstracts/violent-crime-strangers-and-nonstrangers*

The civilized world is mostly a safe place; if you're careful and courteous, and if you pay attention to your actions and surroundings, then there is a very high probability that you'll be safe and secure. This is the optimal frame of mind not just for surviving in the real world, but for browsing the Internet and using your smartphone. We must be careful, however, to avoid becoming complacent in situations and environments that are typically or historically safe. For instance:

- When you're in your car and headed toward an intersection with a green light, look both ways to ensure that cross-traffic has stopped and there are no emergency vehicles approaching.
- Ensure that your garage door is closed, and all other external doors are locked before you leave the house, and before you go to bed each night.
- Treat all firearms as if they are loaded, even if you're *absolutely certain* that they aren't.
- Ensure that your purse is zipped closed, and/or your wallet is not accessible to pickpockets when you're shopping or walking in public.
- Check for mold before buying a carton of blackberries.

All we can do is give ourselves the best chances to stay safe and secure by removing the most common avenues for loss and tragedy. You can't stop someone from driving drunk, but you can watch for erratic drivers and get out of their way. You can't stop hackers from trying to break into your email account, but you can make it extremely difficult and expensive for them to succeed.

Case Study: East Germany

While skepticism is essential for staying safe both online and in the physical world, too much of it will do more harm than good. Consider the lasting social destruction in the ironically-named German Democratic Republic (GDR for short, or more commonly known as East Germany) during its post-WWII Soviet occupation, as documented in the paper: *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany* by

Andreas Lichter, Max Loeffler, and Sebastian Siegloch[6]. As the East German Ministry for State Security (known informally as the Stasi) increased its surveillance and information-collecting on citizens, there was a measurable impact on all of the standard markers of a healthy society:

- Decreased level of trust in strangers
- Increased negative reciprocity (selfishness, greed, thievery)
- Fewer number of close friends
- Less sociability (going to parties, gathering with friends)
- Less volunteering
- Lower participation in local politics

People were pressured into informing on their family, friends, lovers, neighbors, and co-workers to the point that every other human being was viewed as a potential threat to a person's freedom and safety. To give you a taste of what East Germans endured at that time, here's a brief excerpt from a 2019 article in *The Atlantic* titled "The Lingering Trauma of Stasi Surveillance"[7] that documented a moment from a survivor support group:

[6] *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2845286*
[7] *https://www.theatlantic.com/international/archive/2019/11/lingering-trauma-east-german-police-state/601669/*

> *The rest of the group agreed that the destruction of trust was one of the most painful legacies of their experiences in the GDR. The dense informer network meant that everyone spied on one another. Many did not find out who had informed on them until decades later, when they requested their Stasi file. One woman spoke of how she was devastated when she discovered that the man she loved was informing on her. Still reeling from this betrayal, she later found out another close friend was also spying on her. A man at the session recounted how his intention to leave the country was betrayed, and so instead of getting out, he was thrown in jail. Ten years later, on receiving his Stasi file, he found out that the person who betrayed him was his girlfriend.*

There was also a measurable economic impact. The more spying the Stasi did on East German citizens, the higher the level of unemployment, and the lower the level of entrepreneurship and self-employment. Why? Because no one trusted their customers, employees, or bosses. A lack of basic trust necessitated a constant stream of busywork for everyone. The impact of the Stasi's extensive domestic spying efforts was so pervasive and traumatic that it lasted well beyond the fall of the Berlin Wall. Many surviving residents of the former Communist occupation still remain socially disengaged, distrustful, and isolated from their peers more than 30 years after East Germany was liberated.

Resist Pessimism, and Don't Lose Hope

As I write this, the world is increasingly sliding into pessimism and tribalism, and media technology in all its forms is largely both the incubator and catalyst for our shared cynicism. It's not quite as bad as the broken social culture of occupied East Germany, but sometimes it can feel that way. The Stasi is long gone, but the constant dread and fear it inspired can feel familiar to modern media consumers. There is hope, and you are both a source and a benefactor of it.

About the Author: Chris Parker

As a southern California native who grew up at the dawn of the PC era in the late 1970s and '80s, my entire life has been connected to technology and the Internet.

In 1987 I launched a BBS (Bulletin Board System, a text-based, non-Internet online community platform accessible via direct dial-up connection) called The Citidel, enabling techies of the day to share data, news, and messages.

In 2000 I created WhatIsMyIPaddress.com to help people answer a common technical question, and over the next few years it grew to become the number one website in the world for looking up an IP address. Today, WhatIsMyIPAddress.com is one of the top 3000 sites in the United States, with more than thirteen million visits monthly.

In 2020 I observed that the Internet had become a dangerous place. As connected technologies advanced, a constantly increasing number of innocent people were being targeted by hackers, imposters, and online cyber crooks. In response I launched the *Easy Prey* podcast to help educate the public about known and emerging threats to people's privacy and digital security. From the archives of that podcast and with the help of colleagues, I created this book to reach a wider audience.

Other than that, I've been interviewed by ABC News as an expert on avoiding romance scams, a guest on many popular podcasts, and I'm an alumnus of California State University, Fullerton.

Other Contributors

I couldn't have written *Privacy Crisis* without the invaluable assistance of the following people:

Stephan Spencer (www.stephanspencer.com) is an early pioneer of search engine optimization (SEO), online marketing, and a serial entrepreneur in those spaces. He's also the co-author of the bestselling book, *The Art of SEO;* co-author of *Social E-Commerce;* and sole author of *Google Power Search,* as well as a contributor to many industry publications.

Jem Matzan (www.jemmatzan.com) was a technology journalist in the early 2000s; an IT technical writer and information architect for Hitachi

and Intel; and has written, ghostwritten, or substantially contributed to 16 books across a wide spectrum of non-fiction technical topics and fiction genres, including the award-winning corporate IT satire *Try Catch Finally*. He's also an award-winning audiobook producer and voice actor.

Chapter 1: Immediate Actions to Increase Security

Security and privacy are not the same thing, but they are closely related. Security is locking your windows; privacy is covering them with blinds or curtains. Enhancing one inherently benefits the other; obviously if you leave your windows unlocked, you're vulnerable to having your privacy violated by thieves, and if you don't cover your windows, you make it easier for thieves to see if you have anything worth stealing. These two concepts are even more synergistic in the digital realm because your personal and private information is – at least initially – what digital thieves want to steal. Therefore every action you take to enhance your digital security equally improves your ability to protect your privacy online, and vice-versa.

From Chapter 3 onward, I describe the kinds of information that can be collected about you, and how it can be used to your detriment. When you understand all of this material sufficiently, then you'll be better enabled to change your habits and practices to improve your privacy and information security. However, there are some critical actions that I strongly encourage you to take right now to protect yourself against immediate threats:

1. Completely shut-down / power-off your smartphone for at least five minutes.

2. Lock your mobile phone SIM through your wireless service provider.
3. Encrypt all of your computers and mobile devices.
4. Get a zero-knowledge password manager and migrate all of your account credentials and other secret information to it.
5. Freeze your credit files with Experian, Equifax, and Transunion.
6. Enable one or more methods of strong two-factor authentication for your primary single sign-on account.
7. From now on, distrust by default any request for payment or to change the method of payment, no matter who it seems to be from.
8. Don't unlock or use your phone in a crowded place, and never let anyone borrow it.

Each of these actions is explained in the subsections below.

Turn Off Your Smartphone For Five Minutes

Most people understand that **power-cycling** a device (turning the power off, then turning it on again) can resolve strange problems and sluggish performance, but did you know that it can also help keep your mobile devices more secure?[8]

When an operating system like Android, Windows, or iOS is started from a power-off state (also known as a **cold boot**), it runs a set of system checks that validate the functionality of the hardware, and a set of initialization processes that establish memory and storage resources for itself and (separately) for user apps. When a program or app is launched on that operating system, it goes through a similar set of health checks and resource requests for itself. Usually these tests and initialization procedures are only performed when a device is **booted** (when it is powered on or reset).

For various not-completely-understood reasons, when software has been running continuously for a long time, it can begin to malfunction:

[8] *https://www.lifewire.com/turning-off-phone-boosts-security-7553751*

- Apps may fail to adopt configuration changes that were applied during updates or patches.

- Some of the data stored in temporary memory (including RAM and the cache space reserved in permanent storage) can become corrupt. This can be from poor-quality software development, minor hardware flaws, or the unpredictable effects of extreme temperatures (hot or cold).

- Sometimes the firmware or drivers for a specific piece of hardware are flawed in terms of long-term resource management, and need to be reset from time to time.

- Sometimes apps take a certain amount of RAM and storage for themselves, then for whatever reason keep asking for more and more until the device slows to a crawl or the app or the operating system crashes.

- Sometimes an app will use cached data when it should be calculating new data, and there's no way to force it to refresh without rebooting the device.

- Software is often inefficient with how it reserves, uses, erases, and relinquishes control of a device's temporary memory (RAM) and permanent storage.

Temporary memory is very fast in terms of input and output, but it requires a continuous and steady supply of electricity.[9] When the power is cut, everything written in RAM is erased. In theory this should be instantaneous, but in practice it can take anywhere from a few seconds to a few minutes for the memory to fully clear because the hardware will retain a little bit of electricity after it's been powered off.

All forms of modern electronics hardware employ hundreds – or thousands – of components called **capacitors** that act as tiny batteries in various parts of the circuitry, providing a steady source of electricity for larger and more complex components such as transistors and storage chips. Small capacitors generally drain very quickly, but larger ones can

9 *https://www.intel.com/content/www/us/en/support/articles/000092253/wireless.html*

hold a charge for quite a while after a device has been unplugged. High-output stereos, amplifiers, and old-style CRT (cathode ray tube) displays can have capacitors as large as D-cell batteries; before doing any component-level diagnostics on these devices, repair technicians typically connect something to the circuit board (such as an incandescent light bulb) to more quickly drain those capacitors.

Therefore simply restarting a device isn't good enough to clear the data from its temporary memory; you have to completely power it off, then wait a while for the capacitors to drain before powering it back on. For PCs this time interval is about 20 seconds; for mobile devices it may take up to five minutes.

The reason why power-cycling your mobile devices is an important security precaution is: there are certain kinds of **malware** (software designed to cause harm) that can infect and run on your phone by residing in temporary memory.[10] These malicious programs are so subtle that they can be executed in "no click" scenarios; they can infect your smartphone when you open an email sent by the attacker, even if you don't tap or click on anything in or on them. From there, the malware can record your voice calls and other activity, and secretly send it to the attacker. Anti-virus software is not able to reliably stop these kinds of attacks.

Fortunately you're unlikely to be the target of "no click" malware unless you're a political journalist, politician, extremely wealthy celebrity, or are involved in terrorism. That doesn't mean you shouldn't take action to protect yourself:

- Turn off your mobile devices for at least 5 minutes *right now*. If you believe you may be at risk of being the target of a "no click" malware campaign, then the US National Security Agency (NSA) recommends power-cycling your phone every day.[11]

- Never open any suspicious email (even if it's only *slightly* suspicious) on your smartphone or tablet.

---

[10] https://www.lifewire.com/just-looking-at-that-message-could-compromise-your-device-5213874
[11] https://www.usatoday.com/story/tech/2021/07/28/turn-off-turn-on-simple-trick-stopping-phone-hackers/5404110001/

Lock Your Mobile SIM

Every mobile device requires a unique physical or virtual **SIM** (subscriber identity module) chip in order to connect to a carrier. The SIM – not your phone hardware or billing information – identifies you as the sole user of a mobile device. A physical SIM card is intended to be accessible to consumers, and can be easily moved from one device to another, so long as the carrier hasn't made it exclusive to one device (known as **SIM locking**).

Leaving a SIM unlocked is convenient for people who use multiple mobile devices, but only want to pay for one service plan. It's also convenient for thieves who can use a process called **SIM-jacking** to secretly transfer your SIM to a different device, which will enable them to receive your phone calls, text messages, and email without your knowledge (there's more information on SIM-jacking in Chapter 3). If your SIM is locked, though, it cannot be moved to another device without providing the correct PIN.

SIMs can be locked and unlocked at will, but you will need the assistance of your mobile service carrier. Different carriers have different policies for how SIMs are initially configured for new lines of service; some lock your SIM by default, others do not. Locking your SIM (or SIMs, if you have multiple mobile devices) is a simple task. You can usually check your SIM lock status through the carrier's website or mobile app, but you can also call the main customer service number (the one printed on your mobile service bill) and ask a rep to do it over the phone.

If you have not already locked your mobile SIMs, then you should assume that they are currently unlocked. Take action to lock all of your mobile device SIMs immediately to prevent SIM-jacking.

Encrypt Your Devices

The most basic definition of **encryption** is: *the ability to communicate securely in a hostile environment.* For your computers and mobile devices, this means that all data stored on them is scrambled with an encryption scheme so complex that it would take *centuries* for a room full of the world's most powerful computers to crack it. That means thieves, hackers, police departments, private investigators, and even the most powerful **three-letter agencies** (top-level national law enforcement or clandestine services

that are typically known by a three-letter abbreviation, such as the FBI, NSA, CIA, ATF, MI5, MI6, GRU, FSB, or Mossad) in the world are unable to decrypt it without the key. If someone really wants access to your encrypted data, then they'll have to find a way to get the key from you.

Data encryption can be applied in three ways:

- **At rest**: data stored on a device. This includes your device and any remote servers where you store data, such as Google Drive, Dropbox, iCloud, or OneDrive, and third-parties that promise to store your data securely (hospitals, banks, schools).

- **In transit**: data that is being transferred over a cable or network from one device to another. Even if the data is intercepted in transit, it cannot be decrypted without the key.

- **End-to-end**: data is encrypted at rest *and* in transit. Every device and service you use should offer end-to-end encryption, where applicable.

At minimum all of the data stored on your smartphones, tablets, PCs, and laptops should be encrypted at rest; at best, all of your devices and services are end-to-end encrypted. Think about all the sensitive data stored on your devices. Without encryption, a skilled digital thief or dishonest service technician can easily access the storage components on your devices without needing to unlock the screen.

Encrypted data is inaccessible to anyone who does not have access to your decryption key. Just like with two-factor authentication (explained later in this section), there are many key paradigms:

- Biometric factors such as your fingerprint or an image of your iris or face

- PIN or password

- Physical security key that connects via Bluetooth, NFC, or USB

- Mobile device that is configured to perform the functions of a physical security key

- Long string of text characters stored in a file

- 12- or 24-word passphrase
- A temporary alphanumeric code generated by an authenticator app

It's possible to encrypt only some pieces of information on an otherwise unencrypted device (such as the usernames and passwords stored by a password management app), and it's possible to encrypt some pieces of information twice (once through an app, and again by encrypting the device's entire storage component). The most important action to take right now is to encrypt each of your mobile and computing devices so that all of the data stored on them is only accessible to you. By "each of your devices" I mean not just the ones you actively use, but also old smartphones, tablets, and computers that are no longer in service.

Encryption only keeps your data safe when your device is locked or turned-off. If there are major security vulnerabilities in the apps, sites, and services you use, or if you inadvertently install a virus or malware, then some or all of your data may be exposed to remote attackers when your device is unlocked. The best defense against this is to keep the operating systems and software up-to-date on all of your electronic devices. When your devices are no longer supported with security updates, it's time to erase and reset them and replace them with newer models, or with more secure alternative operating systems.

Newer versions of the most common operating systems (Windows, MacOS, iOS, Android, Linux) either encrypt all at-rest data by default, or give you the option of encrypting your device when you go through the first-time setup procedure. Even if you're pretty sure all of your devices are encrypted, it's worth the small amount of effort to verify their security. Here's how you can check for and enable encryption on your mobile and computing devices:

Windows

For Windows 11 devices, go to the **Start** menu, then select **Settings**, then **Privacy & Security**, then **Device Encryption,** then turn on **Device Encryption** if it is not already enabled.

For Windows 10 devices, go to the **Start** menu, then select **Settings**, then **Update & Security**, then **Device Encryption**, and follow the directions from there.

For the Professional edition of Windows 10 or 11, encryption should be handled via **Bitlocker**. Go to the **Start** menu, then select **Settings**, then **Privacy & Security**, then **Device Encryption**, then **BitLocker Drive Encryption**, then (if it isn't already enabled) turn on **Device Encryption**.

As of January 2023, all Windows versions prior to 10 are no longer receiving security updates, and are therefore highly vulnerable to remote intrusion. If you are using Windows 8, 7, Vista, or XP, then you must either upgrade to Windows 10 or 11, or immediately remove all potentially sensitive data from the machine. If you are using Windows 98, 95, or 3.1, then you should return to your native timeline and stop meddling with our temporal reality.

MacOS

On Macs, encryption is handled through the **FileVault** application. To enable it, go to the **Apple** menu, then click on **System Preferences**, then **Security & Privacy**. Select the **FileVault** tab, then click the **lock** icon in the lower left corner of the window, and provide your Apple login credentials. Finally, click on **Turn On FileVault**, then follow the on-screen instructions.

iOS (iPhone, iPad)

If a passcode is set on your iPhone or iPad, then the device is automatically encrypted. To verify this, go to the **Settings** app, then tap on either **Touch ID & Passcode** or **Face ID & Passcode,** and ensure that the **Passcode** option is **On**. If the menu item says "Turn Passcode On," then tap on it and set up a 6-digit passcode.

If you currently have a 4-digit passcode, consider changing it to 6 digits. It isn't that much more difficult to remember, and it takes a *lot* longer for a thief to guess the combination.

Android

The process can differ slightly depending on which version of Android you're using and who the phone manufacturer is:

- Samsung devices: Go to **Settings** (the gear icon), then **Biometrics and Security,** then **Other Security Settings,** then **Strong Protection.**

- Most other Android devices: Go to **Settings** (the gear icon), then **Security,** then **Encryption & Credentials.**

While you're there, ensure that your SD card is also encrypted (if your device has removable storage).

Also, you should revisit your lockscreen settings. Swipe patterns are very easy to observe, both by **shoulder-surfing** (someone standing behind, above, or next to you observing your keystrokes or swipe patterns) and by examining the smudge marks on the screen. PINs are easy to guess, so try to use a unique one for your phone. The most secure methods are biometrics (fingerprints and face recognition).

Google typically only provides security updates for four years for each major Android release. For instance Android 11 was released in September 2020, and its final security patch was delivered in February 2024. Other vendors such as Samsung may offer longer or shorter support terms, but in general they'd rather sell you a new device than continue to support an old one. Make sure you keep all of your devices as up-to-date as possible, and when it isn't possible to upgrade them to a supported Android release, then it's safest to completely erase and reset the phone and trade it in or recycle it, or (if possible) to replace the default operating system with LineageOS (formerly known as CyanogenMod).

Linux

On Linux it's possible to encrypt the whole hard drive, or individual partitions on it. At minimum your `/home` directory needs to be encrypted, so if you didn't encrypt the entire drive by default, then it may make sense to encrypt only the partition it's mounted to.

The best time to encrypt a drive or partition is when you first install your Linux distribution, but longtime Linux users may not have that option if they've continually upgraded from an era when encryption was not part of the installation procedure. To check for encryption on a drive or partition, use a partition manager such as `parted` or `gparted`. Select a partition, then look for the word `LUKS` in its description. From the `parted` command line, the `print list` function will show detailed information about every partition on the drive. Encrypted partitions will look something like this, with `(crypt)` in the `Model` line, and `luks` in the `Disk` line:

```
Model: Linux device-mapper (crypt) (dm)
Disk /dev/mapper/luks-d714a9e4-2ef2-4d93-ab6f-
   5b53a59a457c: 20.0GB
Sector size (logical/physical): 512B/512B
Partition Table: loop
```

Unfortunately there is no way to encrypt a Linux partition while it's mounted (while you're actively using it) as of the publication of this book. That means that you'll have to boot into a live CD or live USB environment, then encrypt your hard drive partitions from there. Instructions for this process are distro-specific, so the best I can reasonably do here is to ask you to engage with your distro's documentation and community support resources to figure out how to proceed. If you aren't able to do that, then you should back up your entire `/home` directory, then wipe the drive and reinstall your Linux distro from the latest ISOs.

Organize and Manage Your Secrets and Papers

How are you currently storing the account credentials for all of the sites, apps, devices, and services that you use? If I were to guess, I'd say you probably mostly use the password management feature of your Google or Apple account (the default methods of storing credentials on Android and Apple smartphones, respectively), and maybe also whatever is built into your preferred Web browser, and possibly you're also using some papers in a desk drawer or sticky notes on your monitor bezel, or you've forced yourself to remember them. A hodgepodge of secrets-management methods like these is, in collective, a poor information security practice.

While your Apple ID or Google account is sufficiently secure for storing usernames and passwords, and for biometric identification (fingerprint, iris scan, face scan) on your mobile devices, it doesn't have the capacity to store your other secrets, such as:

- PINs for various accounts, devices, and cards
- Answers to security questions (this is explained in more detail later in this chapter)
- Bank account and routing numbers

- TSA Known Traveler Numbers (KTNs)
- Credit card details
- Insurance account numbers
- Driver's licenses and license plates
- Social Security numbers
- Dates of birth
- Recovery phrases for cryptocurrency wallets
- Combinations for locks and safes
- Gate codes
- Mobile device IMEIs

While you can reasonably remember many of these things for yourself, you probably can't easily memorize the important secrets for your spouse or partner, children, and elderly family members in your care. And as morbid and uncomfortable as it is to think about this topic, having all of this information handy (while also keeping it secure) will make it much easier for you and your family if something terrible should happen to one of you.

There are also many kinds of less-critical pieces of information that should be stored securely in a digital format, and are convenient to be able to access on demand:

- Membership numbers for clubs and other organizations
- Frequent flier miles or hotel points account numbers
- Employee or student ID numbers
- Utility account numbers
- Vehicle VINs
- Known allergies
- Medications and prescriptions

- Model and serial numbers for expensive electronics, musical instruments, and other valuable items (if any of them are lost or stolen, this information is essential for recovering them)

- Clothing measurements

The point is: you want one "source of truth" for all of the information that is important to you, even if some of it isn't really secret. This way you'll only have to remember one secure password in order to access all of your login credentials, and you'll rid yourself of insecure methods of secrets management such as scraps of paper or unencrypted text files on your computer, on removeable media (CD / DVD, or USB drive), or in cloud storage.

The best secrets-management solutions are usually inexpensive, but never free of charge; they use strong encryption to protect data; and the company or software developers who provide it don't have access to the decryption keys – the technical term for this is **zero-knowledge** because the service provider has absolutely no visibility into the data you store with it, and it cannot possibly access that data under any circumstances because the keys are held only by the end-users. So even if a thief were to copy every hard drive in a zero-knowledge service's datacenter, he would not be able to access any of its users' secrets unless he were to separately steal their decryption keys; similarly, a three-letter agency would not be able to gain access to your secrets without your permission, even with a warrant or subpoena.

Browser-Based Solutions

If you are strictly concerned about usernames and passwords – for instance if you prefer to keep your secrets off of electronic devices, and store them in a safe or bank vault deposit box – then one of the Web browser-based password management tools listed below will be sufficient.

If you are using the Chrome Web browser (on any platform) or an Android-based smartphone, then the **Google Password Manager** is already your default method of safely storing login credentials. Usernames and passwords are stored securely in your Google account, and will be shared across all devices and services that use Google authentication.

The Brave, Edge, and Firefox browsers (each of these is covered in more detail in Chapter 2) encrypt and store user credentials locally on your

computer or mobile device; they are not connected to an online password management service like Chrome is. You can choose to securely share your Brave, Edge, or Firefox password databases among your other devices via the **Sync** feature, but you cannot access your stored passwords outside of the browser.

Migrate to a Secrets-Management Service

A full-featured standalone secrets-management solution is one of the rare instances where *convenience* and *security* align. Typically you'd trade one for the other, but in this case you are better-off storing all of your secrets – not just your login credentials – in a single end-to-end encrypted service. The concept is simple: you create and remember only one secure password in order to get access to a multitude of other passwords and secrets that you can't reasonably remember. Ideally you'll also enable two-factor authentication as well (this is covered later in this chapter).

Legitimate zero-knowledge secrets-management solutions are never free, but they aren't very expensive either. Here are three good, inexpensive secrets-management solutions that I can confidently recommend to you because they are zero-knowledge, have not had major data breaches in the past, and are developed with maximum security and privacy in mind. Take a look at each of them and pick the one that appeals to you:

- **Bitwarden**: https://www.bitwarden.com (A superior option for families or organizations that need to share some or all secrets.)
- **Proton Pass**: https://proton.me (Proton also offers high-quality private and secure email, calendar, cloud storage, and VPN services; as a package deal – which I recommend – this is the most cost-effective option.)
- **1Password**: https://1password.com

By installing the requisite mobile app and browser plugin, your new secrets-management service will replace your current methods of auto-filling login credential fields in apps and on websites, though you may have to change some settings in your browser and on your smartphone (secrets-management services have documentation on how to do this).

Next, you must migrate your account credentials from the old solution to the new one. This is a quick process that the app will handle automatically

for you. Once you've migrated all account information, you should erase it from your previous password manager and ensure that it is no longer the default solution for auto-filling login information.

Audit Your Logins

This is a good opportunity to review your list of online accounts. There have been so many data breaches over the years – and new ones occur several times per day – that you should assume that at least one of your passwords has already been stolen. A good password management utility like the ones mentioned above will have the ability to look for your usernames in a public database of known-compromised credentials, and make it easy for you to visit those old sites so that you can update the passwords. However, it's likely that most of those accounts no longer exist because the compromised sites have been shut down, or the domain name has been sold to someone else and the site's been fully replaced, or the old unsecure software that was breached has been replaced and all of the passwords have been automatically reset. If an account or site no longer exists, you can safely delete the record in your password manager. However if an old, compromised account does still exist on one of those sites, then you must either reset its password or delete the account. Don't delete compromised credentials from your password manager if those accounts still exist!

If you were an early-adopter of computers and online services in the 1980s or 1990s, then you may have more than a thousand accounts to review. Don't get discouraged; this is important, and it can easily be completed on a weekend afternoon or a series of afternoons. Some of the entries will be easy to eliminate because the websites were shut down long ago. For instance if you had an account at the Bear Stearns investment bank (which famously collapsed at the height of the Great Financial Crisis), then you can delete your old bear.com credentials.

You almost certainly have duplicate entries for various subdomains of the same site, or for a website and an app for the same service. For instance you might have separate entries (with identical usernames and passwords) for nfl.com, nflshop.com, sso.nfl.com, and com.gotv.nflgamecenter.us.lite (the low-level technical name for the NFL mobile app). All of these can be consolidated into one canonical record, so long as the login credentials are identical. In rare cases you may discover that you have different logins for the same site, though you only have one account. For instance you might

have stored credentials for youtube.com before it was acquired by Google and subsequently merged with Google's authentication system. Similarly, on non-Google sites you might have chosen to switch from using an older username and password to using a single-sign-on solution such as Google, Apple, or Facebook (which would invalidate your old account credentials).

There will be hundreds of other accounts that are probably still valid, but you may not have used them in a long time; if you know you're not going to use them again the future, and if it isn't difficult or expensive to set up a new account if you do end up needing to use one of those sites again, then it's worth your while to visit those sites or open those apps and delete your account. The fewer accounts you have, the less vulnerable you are to a data breach.

A good password management service will also look for **reused passwords** (using the same password for multiple sites or services) and **weak passwords** (passwords that are easy to guess because they are names or dictionary words, known numbers such as your phone number or social security number, or are simple enough that they can be guessed in a relatively short amount of time by using a password hacking tool). Though it may take some time, it's worth the effort to use the password generator built into your password manager to create **strong passwords** (passwords of maximum allowable length – usually 8, 12, or 14 characters – composed of random uppercase and lowercase letters, numbers, and allowed symbols) for all of your accounts that have weak or reused passwords. Taking this action will exponentially increase the security of your online accounts.

Secure Your Documents and Cards

If your wallet or purse were stolen, you'd probably find out about it within an hour or two. That's enough time for a thief to spend your cash and put a few unauthorized charges on your credit and/or debit cards before you can call and cancel or freeze them. You won't be held responsible for charges incurred on stolen credit cards, but debit charges can cause some extra problems with overdraft fees that can take more time to reverse.

You don't need to carry all of your credit and debit cards with you at all times. At most, you'd need your debit card (in case you need to withdraw cash from an ATM) and one credit card. You don't need to carry more than $100 in cash (and probably less than that, unless you know you'll need

cash for something specific like giving tips to musicians or buying drinks at a cash-only bar). You also don't need to carry any of the following:

- Passport or passport card (unless you're currently in or travelling to a foreign country, or prefer not to use your driver's license for identification purposes)
- Birth certificate
- Social Security card
- Scraps of paper with PINs, passcodes, combinations, or passwords written on them
- ID badges that can gain entry to buildings (unless you're on your way to or from those places)

You must be aware of exactly which cards and other valuable items are in your purse, wallet, bag, backpack, or pocket. Why? Because a professional thief, if given the opportunity, will only steal one item. Since you are unlikely to quickly discover that only one credit card or ID among many is missing – or if you do notice, you'll be more likely to think that you've misplaced it somewhere – the thief has plenty of time to use the card or ID before it's reported stolen. For that reason, if you know you left home with a specific credit card, report it as stolen immediately after you lose track of it. If you did end up misplacing it somewhere, then there's no harm – the bank will send you a new one, with a new number and expiration date, in the mail.

Now consider the various documents stored throughout your home. You might have several desks, filing cabinets, end tables, and kitchen drawers that contain various papers or devices that contain secret or private information such as:

- Everything included in the list earlier in this section
- Tax documents (W2 and 1099 forms, printed tax returns)
- Two-factor security tokens (this is explained later in this section)
- Cryptocurrency wallets and recovery phrases

- Unsecured mobile devices or computers containing private information
- Prescriptions for medication
- Legal documents (wills, judgements, mortgage documentation, summons, subpoenas, contracts, leases)
- Vehicle titles
- Stock and bond certificates
- Bank statements
- Utility and wireless phone service bills
- Keys

A desk drawer containing even a few of these things would be a bonanza for an identity thief.

At the very least, you should consolidate these papers and devices so that you know what and where they all are. Ideally you would store them securely in a fireproof safe, or put them into a safety deposit box at a bank (if they are seldom used). Not only do these methods keep your documents away from thieves, they also preserve them in case of a fire or flood.

Identity thieves don't need to dress like cat-burglars and pry open bedroom windows with crowbars to gain access to your most important documents and belongings. They can be a guest at a party; a date (yours, or one of your teenage kids'); a friend-of-a-friend; a friend of your child's; a neighbor; a coworker; or a tradesman, mover, utility worker, or other service provider who is legitimately in your home to fix, deliver, or install something. By consolidating your important documents and devices and storing them securely in one place (if not in a fireproof safe, then at least in a drawer that can be locked, within a room that can be locked), you'll take away the best opportunities for quick and easy information theft.

Freeze Your Credit

All a thief needs in order to obtain credit in your name is: your full name, current home address, and social security number. With those three pieces

of information, someone can get credit cards, loans, and leases for themselves, and you will be financially responsible for those debts (you can, of course, dispute those debts and eventually have them discharged, but you'll never be compensated for the time and expense involved).

Assume that at least this much of your personal information has already been stolen. There have been more than 20,000 reported data breaches in the US, encompassing nearly 2 billion personal data records.[12] In the 2017 Equifax data breach alone, more than 160 million people's names, addresses, social security numbers, and other personal information were stolen. It would be miraculous if you *weren't* one of those victims, even if you're sure that you haven't yet been targeted by identity thieves.

There is one simple, easy way to protect yourself from credit-based identity fraud: freeze your credit files at the three main consumer credit agencies: Equifax, Experian, and Transunion. All you need to do is go to each of their websites – or install their mobile apps – and, after you've proven that you are who you say you are by validating various pieces of personal information provided by your current and previous creditors, select the option to freeze your credit profile. While all three of these agencies will aggressively push their unnecessary and expensive "credit monitoring" or "credit lock" services on you, you do not have to pay to freeze or unfreeze your credit.

Freezing your credit profiles prevents financial institutions from being able to access them (also known as a **hard pull** or **hard inquiry** of your credit report), which prevents anyone from opening a line of credit in your name. That includes you, so don't forget that you froze your credit; you'll have to temporarily unfreeze it if you apply for anything that requires a credit check: credit cards (establishing new accounts and requesting limit increases on existing accounts), bank accounts, mortgages, leases, cellular phone service, utilities, and some kinds of "background check" services used by employers and landlords. You can temporarily or permanently unfreeze your credit at any time over the phone, through the agencies' websites, or through their mobile apps. When you need to unfreeze, I recommend as short an unfreeze window as is reasonable – one day, at most.

Here are the official website URLs of the three consumer credit agencies:

---

[12] *https://privacyrights.org/data-breaches*

- **Equifax**: https://my.equifax.com
- **Experian**: https://www.experian.com/freeze/center.html
- **Transunion**: https://www.transunion.com/credit-freeze

Enable Two-Factor Authentication

As explained earlier in this chapter, passwords can be guessed or stolen via various methods, so it's unwise to rely solely on login credentials to keep your most important information secure. While many services, platforms, and sites offer a secondary form of authentication – known alternately as **multi-factor authentication** (**MFA** for short) or **two-factor authentication**, (**2FA** for short) – it is not generally required by default. You should enable two-factor authentication whenever and wherever possible.

There are many forms of 2FA / MFA (I'll use those terms interchangeably throughout this book), some are more secure than others, and not all of them are available on every service you use. If you have a choice among several options, here are my recommendations in order from best to worst:

- **Biometric matching**: Using your fingerprint, voice, face, or iris to verify your identity via a mobile device or kiosk.
- **Hardware security key**: (also known as a **hard token**) A small piece of unique hardware that you must connect to your computer (via USB, NFC, or Bluetooth) or mobile device when asked. Alternatively Google enables you to use a spare Android smartphone (not your main phone) as a discrete security key (this is explained in more detail later in this section).
- **Authenticator app**: A smartphone and/or desktop PC app that generates temporary 6- or 8-digit alphanumeric codes that you must type into a text field when asked. The authentication codes typically expire and are regenerated every 30 seconds.
- **PIN**: You may be provided a set of lengthy alphanumeric PINs that you can use to recover access to your account in the event that your other 2FA methods are unavailable (such as if your mobile phone is lost or destroyed). You can store these codes in your zero-

knowledge password manager, or print them onto paper and store them with other papers that you keep secure, such as your Social Security card, birth certificate, and passport.

- **App notifications**: The service may offer an option to validate a sign-in attempt via an app notification on your phone. This is not the same as the authenticator app. For instance, Google will send this notification through the standard Google mobile app, not through the Google Authenticator app.

- **Security questions**: When prompted, you must answer one or more questions that a stranger would find difficult to answer without prior research, such as your first pet's name or your favorite vacation spot. When used as intended, this is a very poor method of 2FA because most security questions are not typically considered secret information. In the next chapter I'll explain how to make this much more secure by using secondary passwords or "dummy information," but for now you should choose better 2FA security methods if possible.

- **Email**: An email will automatically be sent to the email address that you've registered with this service provider. It will contain either a link that you must click, or an alphanumeric code that you must type into a text field when prompted. This method is only as secure as your email account. Most email is not encrypted and could be intercepted in transit, though this is rare for anyone who isn't a high-value target (this is defined and explained in Chapters 2 and 3).

- **SMS text**: Similar to the authenticator app, except the alphanumeric codes are generated remotely and sent to your mobile device via text message. This can alternatively be delivered via an automated voice phone call. If your SIM card is not locked, then this authentication method is not secure. Since SMS text messages are not encrypted, security codes could potentially be intercepted, with the same caveat about high-value targets as email 2FA codes.

Some services may offer several 2FA options; when possible, it's a good idea to enable at least two of them. While I don't want you to catastrophize, you should ask yourself which 2FA methods would be available to you

after a disaster such as a fire or flood. Hardware keys and smartphones can be lost, stolen, or destroyed; if that were to happen, and one of those were your sole method of 2FA, you could be permanently locked out of your accounts. What can you do to ensure that you can securely gain access to all of your accounts if you lose access to all of your devices and papers?

Ideally you would configure at least two of the strongest methods of 2FA for everything you use (bank website, wireless service provider, etc.), but for right now I want you to focus on your password manager or secrets-management service, and the one or two major accounts that you use to sign into most of your apps and websites, otherwise known as a **single-sign-on (SSO)** provider. The most common consumer-grade single-sign-on providers are:

Google

If you have an Android smartphone, then your Google user account is probably your primary SSO solution. You can enable 2FA by going to https://myaccount.google.com, then clicking on **Security**, then following Google's guidance for securing your account with **2FA** and **recovery** options.

Apple

If you have an iPhone, then you're probably using your Apple ID to sign into most things. While 2FA is usually enabled by default, it doesn't hurt to check. Follow the instructions below that apply to your situation:

- **iPhone**: Go to the **Settings** menu, tap your name, then tap **Password & Security**. If it is not already on, then tap **Turn On Two-Factor Authentication**, then tap **Continue**.
- **Mac**: Go to the **Apple** menu, then **System Settings**, then click or tap your Apple ID username. Click or tap **Password & Security**, then **Two-Factor Authentication**. If it is turned off, then turn it on right now and follow the instructions on the screen.
- **Online**: You can also enable 2FA by going to https://appleid.apple.com. Sign in with your Apple ID. If you do not have 2FA enabled, then you'll be asked to upgrade your

account security. Click or tap on **Upgrade Account Security**, then follow the onscreen instructions.

Microsoft

If your computer uses Windows 10 or higher, or if you have a Surface device, then Microsoft's **Windows Hello** service may be the SSO provider you use most. To check your 2FA settings, go to https://account.live.com, sign in with your Microsoft ID, then click or tap on the **Security** tab at the top, then select **Advanced Security Options**, then review the options in the **"Ways to prove who you are"** section. Add new 2FA methods if you can.

Facebook

Many sites, apps, and services beyond Facebook use your Facebook account as an SSO solution. In the Facebook app or on the Facebook.com website, go to **Settings**, then **Security and Login Settings**, then scroll down to **Use two-factor authentication**, then click **Edit**.

> ➢ NOTE: While Facebook (or more broadly: Meta) may be a reasonably safe and reliable SSO provider, it is also arguably the most notorious personal data collector in modern history. If you're currently using it to sign into one or more sites beyond the Meta app empire (Facebook, Instagram, Whatsapp, Threads), then you should migrate to a more consumer-friendly SSO provider such as those listed above.

Secure MFA Solutions

Apps and services have ways of securely trusting your devices such that providing a username and password from a trusted device is sufficient. If you try to log in from an untrusted device or Web browser, or from a different IP address or geographic location, you'll be asked to provide a secondary authentication method. And at certain intervals – every few months, usually – trust must be re-established in the same manner.

Ideally you would be able to choose among many MFA options for the services you use, but lazy service providers will just offer SMS text and/or security questions, and call it a day. Whenever possible, you should use only the most secure MFA methods, and none of the others.

Your biometric ID is good enough for your mobile device, but not every service can access it, and you can only use it if your mobile device is operable and currently in your possession. That doesn't mean it's useless; it just means that you need alternative MFA methods that don't require your primary mobile device.

To supplement biometric ID, two good methods of secure third-party multi-factor authentication are: authenticator apps that provide time-limited alphanumeric codes that you must type or copy when you access a service (so long as they are installed and configured on your other devices), and hardware tokens that you must connect to your device via USB, NFC, or Bluetooth. I recommend both of these solutions; there is no harm in having a hardware security key and also using an authenticator app. Options for each are explained below.

Authenticator Apps

Many popular online services provide their own unique authenticator apps that can be installed on a mobile device. As far as I know they're typically secure, but it can be a real hassle when you switch to a new smartphone because the authenticator may be device-specific, so you might have to deregister the old app, then go through a different 2FA process to register a new one. Some authenticators can be installed on multiple devices.

If possible, rather than deal with half a dozen different authenticator apps for individual services, it's much easier (and no less secure) to use one of the universal authenticator apps listed below (they're all based on the same fundamental technology anyway).

Google Authenticator App

This is free, available for both Android and iOS, and is compatible with a large number of services. Registering new 2FA tokens on it for the services you use is as simple as scanning a QR code.

Authy

https://authy.com/

This is an authenticator app that will work on virtually all mobile and desktop computing platforms. It's similar to the Google Authenticator, but has a few key advantages:

- You can sync your 2FA tokens across multiple devices
- You can backup your 2FA tokens to a zero-knowledge encrypted cloud service
- It works on PCs as well as mobile devices
- It's more secure because it requires its own authentication separate from your mobile device

To clarify that last point: most authenticator apps rely on your mobile device's lock status to grant access. Your phone's storage is encrypted while it is locked, but when you unlock it with a PIN or biometric ID, you – or someone in possession of your unlocked phone – can freely access your Google Authenticator app on it. Authy requires its own password, so if someone were to steal your phone while it was unlocked (or if they guessed your PIN), he or she would not be able to access your 2FA tokens without knowing the Authy password. You should not store your Authy password in your password manager unless the password manager also requires its own unique password or biometric ID; if your password manager requires MFA from Authy, and the Authy password is stored in the password manager, then you've created an inescapable catch-22 unless you have other MFA methods that you can use to get into the password manager.

Authy is another rare example where "security" and "convenience" aren't mutually exclusive. If your mobile phone is lost or destroyed, the 2FA tokens stored in the Google Authenticator app on it cannot be recovered; you'll have to re-establish new tokens on a new Google Authenticator on your new device. Similarly if you have the Google Authenticator app on your smartphone and your tablet, there is no way to share tokens between them.

The only downside to Authy is that it isn't quite as easy to set up as the Google Authenticator. However, the Authy website has excellent documentation that explains how to get it to work with dozens of supported apps and services.

Authy is free to use, and is developed by Twilio, a software engineering services company.

FreeOTP

https://github.com/freeotp

This is an authenticator app with similar features to Authy. The main difference is that it's open source software, so if you run an obscure operating system like OpenBSD or an old version of Android, you can theoretically compile a binary for that platform if you have some basic programming skills.

Hardware Security Keys

Hardware security keys are the easiest and quickest secure MFA solution, but you must have your key with you when you need to use it, it must be able to interface with the device that is requesting it, and it can of course be lost or stolen. For those reasons, I recommend buying two security keys that connect in different ways – such as USB-A and USB-C – so that you can use them anywhere. For maximum security, you should keep one of your keys in a fireproof safe or bank deposit box.

If you lose a hard token, you can disable it remotely through the service provider, then order a replacement. Even if a thief were to steal your key, though, he would still need to know your username and password for each service he wanted to break into.

The most popular and trustworthy consumer-grade hardware key provider is **Yubico**:

https://www.yubico.com/products/

Yubico is based in Sweden, and manufactures its Yubikey products in both Sweden and the US.

Google has offered a few different generations of its **Titan** security keys over the years:

https://store.google.com/product/titan_security_key

Originally Google sold a rebranded USB-A / NFC key made by Yubico, and a Bluetooth Titan key made by Feitian, which is a Chinese company. Absolutely avoid all hardware keys made in China. (I'll explain why this is important in Chapter 2.) After public pressure Google discontinued its Chinese-made keys, and began offering a rebranded USB-C Yubikey instead. Unfortunately this version of the Titan key does not work with all of the same services and software as its Yubikey sibling, so if you're going to get one or the other, I suggest getting a pair of Yubikeys. The only reason to consider buying the (cheaper) Titan key pair is if your primary motivation is participating in Google's **Advanced Protection Program** (though you can use Yubikeys with this service instead of Titan keys). You can find out more about that on Google's official product page:

https://landing.google.com/advancedprotection/

Distrust by Default All Requests For Payment

Scams are constantly evolving. The stories scammers tell are always attuned to modern culture, and their methods of money transfer migrate rapidly to new mediums that are carefully selected for maximum success.

I'll go into detail on scam detection in various parts of this book, but for right now you can ensure your safety by remembering one universal rule: assume that all requests for payment are scams, no matter whom it seems to be from, or how urgent it may seem. Scammers most often pretend to be people you know and businesses you trust, or authority figures whom you'll submit to without question. Here are some examples:

- If you get a text message from your boss asking you for the account details of your company credit card, don't respond. Instead, talk to your boss in person, or at least verify that the request is legitimate through other means.

- If you get an instant message or text message from your spouse or partner asking for your bank account details, don't reply. Instead, call him/her to validate that he or she is in possession of his or her

phone, then provide the information once you're sure it's a legitimate request.

- If you get a call claiming that you owe money to the IRS, hang up. As I explained in the Introduction, the IRS does not make calls like this.

- If you get an email asking you to pay your cell phone bill, delete it. You already know when your bill is due and how to safely pay it. Rather than reply or click on anything, go to your Web browser and log onto the service provider's official website the way you usually do. Links in email can look legitimate at a glance, but actually lead to a scam site.

- If you get a call from someone claiming to be a police officer or lawyer asking you to wire money to bail a friend or relative out of jail, hang up. If it were real, you'd hear from that friend or relative directly. Sometimes this is a two-part scam where someone claiming to be a friend or relative will call and ask for bail, then a second scammer will call a few minutes later claiming to be that loved-one's lawyer. Do not provide any information, or any hints that would give the scammer an advantage (such as guessing the person's name, or asking why they aren't in school). Hang up, this is a scam.[13] If you're really worried, then call that person directly, and/or contact someone else who can verify that the friend or relative in question is not in jail. You can also directly call the police department where they claim to be detained (call the official number, though, not the one that is given to you by the caller). Even if you can't immediately verify the person's whereabouts, assume this is a scam until proven otherwise.

- If you get a call or text message from someone claiming to be a health care worker or hospital administrator, asking you to send money to pay for a loved-one's emergency care, hang up. This is a scam, it is *never* legitimate.

- If you get a call from anybody, do not provide any information to them, even your date of birth or marital status. If you think it might

[13] *https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money*

be important – such as your doctor's office calling for your Medicare account number – then hang up and contact the office or business through a method that you know to be legitimate. Do not call the number that the caller provides to you. You must always initiate contact through official communication channels.

Sometimes a request for payment is not a scam, but you still must verify it by initiating contact with the company or debtor making the request. For instance sometimes utility companies or other monthly service providers are sloppy in their "paperless billing" practices, and will send legitimate emails requesting payment, though the domain name in the link they provide does not match with the company's legitimate website, and the link to the payment portal leads to an unfamiliar domain. This happens for two reasons: the link is being tracked to see if you clicked on it, or a third-party payment processor is handling the account. While in some cases these links may be safe and the requests may be legitimate, **don't take the risk** – don't click the link, don't call the provided phone number, instead delete the email and use the methods you usually use to contact this organization.

When in doubt, request that the information be sent to you by physical mail, but do not provide your mailing address; legitimate creditors already have your mailing address, and they are obligated by Federal law to notify you in writing when they are attempting to collect a debt. This includes the IRS.

Again, for emphasis: assume that all requests for payment are scams, no matter whom it seems to be from, or how urgent it may seem.

Don't Let Your Phone Get Stolen

Modern smartphones have become so expensive that their parts (especially screens and camera lenses) are valuable enough to encourage smartphone theft. If your locked and encrypted phone is stolen, you're out one smartphone, but its replacement cost is likely the extent of the damage. However, many of the precautions I've asked you to take can be undone if a thief gets hold of your unlocked smartphone, or is able to unlock it. Thieves have two methods for breaking into locked smartphones:

- Shoulder-surfing to learn your PIN, pattern, or passcode, then stealing the phone via traditional pickpocketing.

- Directly snatching an unlocked phone from the victim's hands while they're using it; thieves often do this from sidewalks while on electric scooters or bicycles.[14]

Don't use your smartphone in a crowded public place where a thief can easily operate. If you must use it and can't duck away into a more private place, then try to put your back to a wall and be extremely wary of the people around you. Also, don't make your PIN or passcode easy to guess; assume that thieves already know your Social Security number, birthdate, anniversary, ZIP code, and ATM PIN.

[14] *https://www.ft.com/content/26be349d-4717-4815-a221-a749e29de2b2*

Chapter 2: Other Important Security Measures

In the previous chapter I explained the immediate actions that you must take to increase your information security. The actions in this chapter are not any less important than those mentioned earlier, but they aren't as critical in terms of immediately securing your personal information. In other words: you don't have to do any of these things *right now*, but you must do them *soon*. If you don't, then you're at risk of being victimized by thieves, hackers, marketers, and disinformation providers. So if you want to skip or skim this section and return to it later when you have the time to complete these tasks, that's fine – but don't forget to come back.

Avoid Chinese Devices, Apps, and Services

The **Chinese Communist Party (CCP)** is notorious for forcing Chinese companies to build **backdoors** (secret methods of remotely circumventing authentication in a device or service; backdoors are covered in detail in Chapter 3) into its products and services. Though there are no official statements or other reliable sources to confirm exactly what the CCP's motives are, we can infer from the results of its long history of anti-privacy practices and digital espionage efforts that its primary goal is to spy on its

own citizens (whether they live in China or elsewhere), and its secondary goal is to spy on foreign governments and corporations. As I explain in Chapter 5, though, even if you are rather boring and unremarkable and don't have access to secrets that the Chinese government wants, you can still be targeted by foreign agents for a variety of reasons.

The worst offenders in the hardware space are: **Huawei**,[15] **Xiaomi**,[16] and **ZTE**.[17] These device manufacturers have been caught including back-doored software in the past, and some of their products may also include backdoors built directly into various hardware components. Absolutely avoid all products made or distributed by these companies, no matter how cheap, powerful, or convenient they may seem.

That doesn't mean that all other Chinese companies get a pass. Any Chinese entity is at risk of being forced to spy on its customers or users, and it can be extremely difficult to detect backdoors in closed-source apps and operating systems, and in low-level device components. The US Department of Commerce maintains an **entity list**[18] of known-untrustworthy manufacturers of electronic devices, components, and software. As of the publication of this book the entity list includes more than 600 Chinese companies, though many of them are on the list for various other reasons not related to personal information collection or backdoors.

On the software side, any app developed in China, owned by a Chinese company, or known to rely on Chinese-controlled resources (such as data storage, data processing, or customer service) is by default untrustworthy and should be treated as a security risk. Of particular note in the software

---

[15] https://arstechnica.com/information-technology/2021/09/security-audit-raises-severe-warnings-on-chinese-smartphone-models/
[16] https://theweek.com/articles/748176/chinese-smartphone-spying
[17] https://www.forbes.com/sites/roslynlayton/2022/12/28/as-china-tech-crackdown-continues-dont-overlook-the-danger-of-lenovo/?sh=1a7c0de05d72
[18] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

space are **TikTok**[19][20] and **WeChat**[21], both of which are known to collect a wide variety of private information from users, and to make that data available to certain employees upon request. If these apps are on any of the devices in your household, stop using them immediately and uninstall or disable them.

While the CCP considers Taiwan part of its sovereign territory in theory, in practice Taiwanese companies are not currently (as of the publication of this book) subject to the CCP's demands for backdoors and private data access. Therefore hardware and software made in Taiwan are inherently more trustworthy than those created by companies based in mainland China, though that may change in the future if the CCP usurps Taiwan's sovereignty through force.

Secure Your Data Transfers

To maximize privacy and security, all data transferred from or received by your electronic devices must be encrypted. I've already explained how to encrypt the data stored "at rest" on your devices, and I've explained that you must vet your service providers to ensure that they use strong zero-knowledge encryption for any of your data that they store. Now it's time to ensure that your data is secure **in transit** between your devices and your service providers. There are three aspects to this:

1. Encrypting all data that transmits over a network.
2. Stripping personally-identifiable information out of all communication that, for whatever reason, cannot be encrypted.
3. Preventing others from secretly using your wireless networks and snooping on you.

The following subsections explain how to ensure that your online communication is safe.

---

19 *https://web.archive.org/web/20200506065834/https://www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china/*

20 *https://web.archive.org/web/20200410180937/https://www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html*

21 *https://securelist.com/hz-rat-attacks-wechat-and-dingtalk/113513/*

Web Browsers

Every Web address you ever visit should begin with `https://` instead of `http://`. The 's' is short for *secure,* which means that all information transmitted between your browser and the website you're accessing is encrypted via the **Transport Layer Security (TLS)** protocol. If you encounter a URL that starts with `http://`, don't click on it. Instead, you could copy and paste it into your browser, and add the 's' manually, but it's better to configure your Web browser to do that for you.[22] Instructions for each major browser are included in the subsections below.

> ➢ NOTE: As of version 15, the **Safari** browser automatically applies HTTPS to all URLs; it does not require any configuration. The **Brave** browser (which we cover later in this chapter) automatically forces HTTPS by default, and doesn't offer the option to disable it.

Chrome

Go to the **main menu** (the icon with the three vertical dots in the upper right corner of the window), then select **Privacy and security**, then **Security**, then ensure that the option for **Always use secure connections** is toggled on (the slider is pushed to the right, and is not greyed-out).

Firefox

Go to the **main menu** (the icon with the three horizontal lines in the upper right corner of the window), then select **Privacy & Security**, then ensure that the option for **Enable HTTPS-Only Mode in all windows** is selected.

[22] *https://www.eff.org/https-everywhere/set-https-default-your-browser*

Edge

As of the publication of this book, Microsoft Edge hides the **Automatic HTTPS** feature from its menus, but you can still enable it by going to this URL in your Edge browser:

```
edge://flags/#edge-automatic-https
```

Change the drop-down box next to this setting from **Default** to **Enabled**, then click the **Restart** button in the lower right corner of the window.

Email

I have some advice and recommendations for you on how to select a good email service provider later in this chapter, but for right now I want to ensure that whatever email service you're currently using is configured for privacy and security.

At the very least your email service should use TLS by default. Webmail-first services such as Gmail and ProtonMail[23] rely on HTTPS for secure communication via your Web browser, which encrypts all data in transit. However, this does not apply if you choose to use a local email client instead, such as Outlook, Thunderbird, KMail, or Evolution, because they use a different set of protocols that are specific to email.

> ➢ NOTE: By default, Apple Mail uses TLS for sending and receiving email.[24]

If you're using an email app other than Gmail (which is a Web app, and therefore uses HTTPS) and Apple Mail, check the account or server settings to ensure that you are using the **IMAPS** protocol (again, the 'S' stands for secure; don't use regular IMAP without the 'S') for receiving email, and that **TLS** is enabled for sending email via the **SMTP** protocol. Do not use the POP3 protocol; it is not secure.

The server settings for all email apps are nearly identical, so I'm only going to provide the specifics for Microsoft Outlook, and trust that you can modify them for whatever email program you're using. In Outlook, go to the **File** menu, then select the **Info** tab on the left, then **Account Settings**,

[23] *https://proton.me/blog/email-is-your-digital-id*
[24] *https://support.apple.com/guide/security/tls-security-sec100a75d12/web*

then **Server Settings**. In both the **Incoming Mail** and **Outgoing Mail** sections, ensure that either **SSL/TLS** or **STARTTLS** are shown in the **Encryption** fields. If neither option is shown there, then you must contact your email service provider to learn how to modify the server and port settings to enable **TLS**. Alternatively (preferably) you should strongly consider moving to a privacy-first email provider, as explained later in this chapter. While it's nice that you have the option of enabling greater privacy and security, in my opinion these should be mandatory features built into all service providers and email apps.

Always Use a Virtual Private Network (VPN)

While TLS will protect all data that you *consciously* exchange with Web and email servers (such as your login credentials, email messages and file attachments, and anything you type into text fields on a website), a much larger volume of information is passed behind the scenes. Basic communication requests – such as when your browser initially connects to a website, and whenever it makes a request for a resource such as an HTML file or an image to display – are **in the clear,** meaning they are not encrypted. Also, your **Internet service provider (ISP)** or wireless carrier can record all unencrypted information such as the URLs of the sites you visit, and the filenames of images and programs that you download. They can then use this data in various ways: to selectively throttle your data usage (such as limiting your video streaming or gaming data speeds), for targeted marketing / advertising, or to sell to other companies that will use it to manipulate you with ads, spam, and mobile push notifications.

An ISP can also be compelled to report potentially illegal activity to law enforcement, such as visits to terrorist propaganda sites; downloads that appear to be child pornography; or Web searches for the purchase or manufacture of narcotics, murder-for-hire services, instructions for creating explosives, or abortion services in states and nations where abortion is illegal. You don't need to intend to commit crimes or acts of violence to be reported to law enforcement; you could be researching any of these topics for a book or paper you're writing, or simply be curious about them.

When your devices (smartwatch, smartphone, tablet, laptop, desktop PC, etc.) connect to a website or other Internet-connected service, they freely reveal quite a lot of personally-identifiable information such as your browser version, operating system, hardware information, date and time

of your visit, geographic location, and these two archaic pieces of technical data:

1. Your device's **Media Access Control (MAC) address** (the string of characters that represents the network chip or modem built into your mobile device, PC, network router, and all "smart" devices)

2. Your **Internet Protocol (IP) address** (the string of characters that your ISP and/or network router assigns to every device that connects to it)

MAC addresses are hard-wired into every modem and network chip, and cannot be changed. However, it is easy to create a fake MAC address (known as **MAC address spoofing**) through your device's operating system; Windows 10 and above, Linux 3.18 and above, and Android 6 and above all have methods for generating new spoofed MAC addresses so that you're never sending out your actual hard-coded identifier to your Internet service provider. That doesn't mean your connected devices are *impossible* to track, but it would take the technological resources and political powers of a three-letter agency to work around spoofed MAC addresses.[25] Unless you're involved with international terrorism, political corruption, espionage, organized crime, human trafficking, or money-laundering, you don't have to worry about this.

IP addresses can be either **static** (permanently assigned to a specific device until it is manually re-assigned to a different one) or **dynamic** (auto-generated at intervals and randomly assigned or re-assigned to connected devices). A static IP address is directly traceable to a specific MAC address in a specific location, and therefore to that device's owner. This isn't inherently bad; websites, for instance, must have static IP addresses so that domain name services know which server to direct traffic to for a given URL. Typically you would not want to have a static IP address unless you were running a server out of your home or office – and anyway, it costs extra and there's no reason to pay for it if you don't need it.

The majority of people are using Internet service providers that assign dynamic IP addresses to customer devices through a protocol called **Dynamic Host Configuration Protocol (DHCP)**. Each ISP has its own policy for when dynamic IP addresses are reassigned, but typically it is

[25] *https://superuser.com/questions/802421/can-a-website-see-know-my-mac-address-even-if-i-use-a-vpn*

every time a device requests a new connection (such as when you restart your computer), or every seven days. Most ISPs keep logs of all of the sites and services each customer uses, and may be compelled by law enforcement to provide those logs upon request. While website owners and mobile app developers may be legally limited in their ability to profile you based on your IP address, ISPs are rarely required to adhere to the same laws and regulations; you should assume that your ISP knows everything you do online unless you encrypt all of your network traffic by using a **virtual private network (VPN).**

The easiest and safest way to obscure your IP address and prevent your ISP from recording your network activity is to use a virtual private network on every device that connects to the Internet. VPN services act as intermediaries between your devices, your ISP, and the sites and apps that you connect to. Rather than revealing your IP address to the public Internet, the VPN substitutes one of its own IP addresses from one of its datacenters. The best VPNs will also encrypt all of your data in transit so that no one – not even your ISP – can secretly monitor and record what you're doing online, filter out ads and tracking code that marketers and data brokers embed in websites and emails to secretly identify you and your activity, and won't keep any logs of user activity (so that there are no meaningful records for hackers, law enforcement, or three-letter agencies to steal or subpoena). VPNs can also enable you to make it look like you're someplace else. For instance if you are prevented from visiting a site or using a service because it is prohibited in your state or nation, or if you're region-locked into a certain sports market and want to watch game broadcasts from some other region, a good-quality VPN will enable you to do that.

Despite all that a VPN can do, it is vastly less complicated to use than you might expect. There's no hardware to buy or elaborate command-line utilities to run; a VPN is just a program that you run on your computer, tablet, or smartphone. You can choose to run it automatically when your device boots up, or you can turn it on and off manually.

There are dozens of VPNs on the market, but many of them (especially the "free" ones) do not provide all of the protections that I've mentioned in this section – particularly the recording of user logs. Fortunately, good, privacy-focused VPNs are not expensive or difficult to use. Here are a few that I have personally evaluated, and confidently recommend:

- **ProtonVPN:** https://protonvpn.com/ (This is part of the highly-recommended Proton family of privacy-focused services that include secure email, file storage, calendar, and secrets management.)
- **Brave Firewall + VPN**: https://brave.com/firewall-vpn/ (This is closely associated with the privacy-focused Brave Internet browser, which is covered later in this chapter.)
- **NordVPN**: https://www.nordvpn.com
- **SurfShark**: https://www.surfshark.com

Lock Down Your Wireless Networks

Your ISP can individually identify you as a customer because you are paying for the service account associated with your broadband modem or cellular device. That doesn't necessarily mean that you or your family have exclusive access to your Internet service. If your wireless router is old or isn't secured, anyone within range can use it to get on the Internet via wi-fi. Fortunately your ISP is also able to identify individual devices that connect through your modem or router, so you'd probably be exonerated if the FBI showed up at your door asking why you were searching Google for instructions on how to make bombs and fake passports; you'd be able to prove that the MAC address of the device that executed those queries was not associated with one of your devices. It's best not to take that risk, though.

Unfortunately I can't offer specific instructions for securing every wireless router and wireless broadband modem. What I can do is encourage you to make configuration changes so that every device that offers wi-fi access in your home (and also your car, if it has a built-in wi-fi hotspot) is secure:

- **Must require strong authentication in order to gain access.** This means at least 256-bit SHA encryption, and a randomly-generated (by your password management app) password no fewer than 12 characters in length. If your wireless router only supports older standards (such as WEP), you must either update its firmware (if possible) or replace it with a new one.

- **Restricts access only to the MAC addresses of your devices** (phone, watch, TV, tablets, computers, etc.).

- **Does not use a default password or generic login credentials**, both for wireless access and for the device's admin or control console. Older routers, in particular, shipped with factory-default credentials for the admin console, and many people never change them. To break into an unsecured wireless router, all you have to do is connect to it, then go to the default admin console local IP address (usually 192.168.0.1 or something similar), and search Google for the default credentials.

- **Must prohibit wireless access to its built-in Web-based management framework**, if possible. Most modems and routers can restrict access to their control panels / admin consoles to wired (physical) connections only, which requires a proper computer with an RJ-45 10/100/1000 network port.

Remove All Publicly-Viewable CVs or Resumes

Job listing sites such as Indeed, Dice, and Monster are data collectors, data brokers (these terms are defined in Chapter 3), and advertisers; they collect as much personal information as they legally can, then they use it in various ways to make a profit at your expense. Largely their data consists of answers to job survey questions, information revealed in online job applications, and the content of users' CVs or resumes, which typically contain quite a lot of valuable personal information: work and school history, home address, phone number, and email address. For the most part, job-listing sites reserve showing this information to hiring managers and recruiters for a fee, but some may list part or all of people's resumes on the public Internet. There is no way to reliably verify that someone is a legitimate job recruiter, though; anyone can pay the fee and gain access to a user's resume and any other personal information the service collects and sells. If you've posted your resume anywhere on the Internet, take it down immediately, or at very least cleanse it of as much personal information as possible.

During times of high or rising unemployment, there is a commensurate increase in employment-related scams. A thief will contact a job-seeker with the promise of a "too good to be true" job offer (for instance: a very

high salary for part-time work that can be done remotely), and ask them to fill out a job application. The application is then used to steal the job-seeker's identity and apply for credit in their name, and/or to transfer money out of their bank account. The only information you need to give a prospective employer or recruiter in an initial application or interview is your name, location, work history, and a reliable method of contacting you. If you're offered a job, however, you will have to securely provide your Social Security number for federal tax and citizenship or visa verification purposes; this should always be done via IRS form I-9 (either on paper or via secure Web form or PDF). You'll also have to provide some method of receiving payment, which you should ensure is securely stored. In pre-COVID times, most job interviews were in person at the company office, so it was easy to verify that both the company and the job were legitimate. In the modern work-from-home world, though, you must be extra cautious when giving out your resume, filling out an application, and finalizing a job offer. Here are some questions you should ask:

- Is the company real? Does it have a legitimate website with investor information, a phone number, and at least one "contact us" email address that uses the company domain name?

- Is this person an employee of the company? Is the official company domain name in their email address (for instance, an offer from Apple would come from `@apple.com`).

- Does the job you're applying for seem realistic for the company offering it, in terms of title, seniority, salary, benefits, location, and workload?

- If this person is a third-party recruiter, which agency do they work for, and who are their clients?

- How much can this person tell you about the job, the company's culture and history, office policies, the work you would be doing, and the products and services that you'd be working on?

- How will your job application be disposed of when a hiring decision is made?

LinkedIn is also a data collector, data broker, and advertiser, and though it does offer job-finding services, it's best described as a social network rather

than a job-listing site. Many professionals find great benefit in the ability to connect with co-workers and colleagues on LinkedIn, but even the most die-hard power users should be very stingy with the information they share with it. LinkedIn's sloppy security practices led to a data breach in June 2021 that exposed personal and private data from about 93% of its userbase – 700 million account records.[26] That data was promptly put up for sale on the **Dark Web** (an alternate implementation of the World Wide Web that uses encryption to protect the privacy of both owners of and visitors to the websites hosted on it; while the Dark Web is not inherently evil, it is often used by criminals to sell illegal drugs, fake passports, pornography, and stolen data).

LinkedIn certainly isn't alone – there have been thousands of data breeches at thousands of companies exposing billions of records of personal information – so on its own, this isn't a good reason to delete your account. You should make your LinkedIn profile private, though, and only connect to people whom you actually know. If you must list your phone number, if possible make it a landline phone or **VOIP** (voice over IP, an Internet-based telephone service such as Google Voice), not your cellular phone. For maximum safety you should not reveal your current employer; as I explain in Chapter 4, innocent people are often mistakenly targeted for vigilante justice, and employers don't always care whether the people they reflexively fire are innocent or guilty.

Purge and Configure Your Google Account

Nearly everyone has a Google account, whether they realize it or not, and it likely contains a lot of personal and private information that can be used against you. If you use any of these Google products, then you have a Google account:

- Gmail
- YouTube
- Android
- Any other Google service that requires a login to use

[26] *https://www.consumeraffairs.com/news/linkedin-data-breach-puts-700-million-user-records-at-risk-062921.html*

By default all Google accounts are maximally permissive in terms of data collection, and minimally secure. Fortunately it's easy to make a few changes to protect your privacy:

1. Log into your Google account at: https://myaccount.google.com
2. Click on **Data & Privacy**, then review each item to see what information Google is collecting and how it is using it.

I advise you to prohibit or limit all data collection as much as possible. The only consequence to doing this is that some personalized features of Google services won't work anymore. It also won't be possible for Google to help find your Android phone if it is lost or stolen.

While you're there, don't forget to enable at least one form of multi-factor authentication for your Google account.

Cleanse and Lock-Down Social Media Accounts

Social media profiles, posts, and comments are a gold mine for thieves, hackers, and marketers. Not only do social media services make it easy to harvest personal and private information, but – as I explain in Chapters 4 and 5 – in general they are <u>not</u> good for you. Ideally you'd permanently delete all of your social media accounts because of the inherent risks to your privacy, mental health, and physical safety, but I know that's too big an ask for the average reader – almost on the same level as asking a smoker to give up tobacco – so the next-best option is to lock down your accounts so that there is as little publicly-accessible personal information as possible, and to remove any information that could be used against you in any way – not just by bad actors, but by social media companies and their "marketing partners."

It's useful to ask yourself why you are using each of the social media services you're signed-up for. If you are using Facebook strictly to stay in touch with friends and family members, then you can pare down your Facebook account to the absolute minimum without sacrificing anything. If the only reason you're on X is to learn about breaking news, then you should consider subscribing to a high-quality politically-neutral (to the extent that you're comfortable with) news service instead, such as *The Financial Times, The Economist, The Associated Press,* or *Reuters,* and your local newspaper.

Regardless of your reasons for using social media services, there is much you can do to limit the real and potential harms intrinsic to them. First, as I advised in Chapter 1, enable the strongest methods of multi-factor authentication. Next, remove as much of your personal information from your user profile as possible, even if it isn't visible to other users:

- Your middle name
- Your maiden name (if applicable)
- Date of birth (Facebook asks for it, but, as I explain later in this chapter, you don't have to tell it the truth)
- Email address (unless you use an anonymized email address from an email service like ProtonMail, which is explained in more detail later in this chapter)
- Employer
- Phone number
- Home address (a PO box is okay, though)
- Location data in photos, comments, and posts
- Relationship status: both in terms of romantic relationships, and family relationships (for instance, don't identify your mother's profile as your mother; thieves would love to know her maiden name)
- Schools you attended, and when you graduated
- Photos of things you own, and of the interior of your home
- Photos of your children

Basically: reveal as little about yourself as possible. If you can stomach it, you should remove all but one simple photo of yourself as well (or at very least, restrict your other photos so that only friends can view them). When thieves and disinformation peddlers create fake social media accounts, they use real people's photos that they copy from real social media accounts. You can do your part to make their work more difficult by reducing your publicly-viewable photos down to one simple profile picture.

Next, make your social media profiles and pages "private," or viewable only to your current connections, then audit your list of connections – friends, followers, etc. If a thief were to hack into one of those people's accounts, what would he or she be able to learn about you? The fewer connections you have, the safer your private information is from thieves, however I want to make it clear that personal and private information should never be considered "safe" if it is on any part of a social media service – even the account information that only the social media company's employees are supposed to have access to. Every bit of information you reveal to a social media company will be used to influence you with ads, offers, suggestions, and algorithmic fine-tuning that alters what you see in the content feed.

Lastly, you should purge every piece of social media content – including Likes, follows, retweets, check-ins, etc. – that you can stand to get rid of. As I explain in Chapter 3, thieves, marketers, and data brokers are masters of tricking people into giving away personal information. Social media makes it extremely easy for them to succeed. Even the act of "Liking" a Facebook page can reveal enough information to successfully manipulate, influence, or steal from you.[27][28] To many readers of this book, this probably sounds crazy – or at least unrealistic – so I've crafted a brief fictional case study that includes several things that individually occur thousands of times per day to normal social media users.

Case Study: Liking Your Way to Bankruptcy

Let's say you have a checking account at a predatory financial institution named Example Bank. Of course it does not *appear* to be predatory; it has its name on a professional baseball stadium, and it runs whimsical TV commercials featuring celebrities and a cute animated mascot. But – as I show in another case study in Chapter 4 – pretty much all big commercial banks are predatory in one way or another, at one time or another. Anyway, let's say you have an account at Example Bank.

Example Bank sends you an email that offers you guaranteed approval for a Visa credit card with a 0% interest rate for the first six months, but only if you Like the bank's official Facebook page. What a deal – all you have

[27] https://www.ft.com/content/555516d4-3d77-11e6-9f2c-36b487ebd80a
[28] https://www.theverge.com/2014/6/28/5852652/facebook-altered-689000-users-news-feeds-for-a-psychology-experiment

to do to borrow money for free for the next six months is click on the "Like Us" button! But if you follow through on this, then you're revealing several things about yourself to Example Bank:

- You are someone who opens, reads, and responds to marketing emails
- You have a Facebook account and can be coerced into clicking the Like button
- You are incentivized to overspend for the next six months

Since Likes are public, and since there is no other good reason for people to click Like on Example Bank's Facebook page, you're also telling thieves, Facebook, and other marketers those same three things, plus another three:

- You have an account at Example Bank
- You have a Visa credit card
- You have a lot of available credit

Let's say you take that deal. Two months from now, Example Bank sends you a "Special Offer" from one of its "partners:" get a 12-month gym membership for the price of only 8 months if you charge it to your Example Bank Visa card. "Wow," you say to yourself, "How did they know that I've been considering going back to the gym? This is a great bargain!"

Let's say you take that deal, too. Two months later, Example Bank sends you another email that offers to send you a FREE "I heart Example Bank" t-shirt… and if you wear it and post a selfie to your Instagram account, the bank will extend your 0% interest rate for another six months.

Shortly thereafter, Facebook starts showing you ads for a "once in a lifetime sale" on a limited edition Fender guitar that you've always wanted; Netflix offers you a half-price deal to re-activate your subscription; and Dell snail-mails you a personalized offer to replace your 5-year-old PC with something twice as powerful for only $1499 – a $250 discount for Visa cardholders. Oh – and if you use your Visa card, your warranty will be extended by up to two additional years (some exclusions may apply).

By the time your year of free borrowing is up, your Visa card balance is $4000, and it's now being charged 30% interest, compounding monthly. It'll take time and a lot of wasted money to pay that down, but wait – here's an email from National Bank of Usury, offering a balance transfer deal: apply for the bank's branded MasterCard, and transfer up to $4500 to it from your Visa card for a flat fee of 2% of the amount transferred, and no interest for 12 months.

While you're applying for the new card, you get a text message on your smartphone: "This is Example Bank. We recently detected unusual activity on your account, and have suspended your charging privileges. Please call this number to unfreeze your account." Oh no! You call the number and talk to an agent, who asks you to verify your home address, social security number, and checking account number. Because you haven't read *Privacy Crisis* yet, you eagerly hand over all of this information, and are told that your account is now ready to accept charges again. Phew! The next day you discover that your bank account has been drained; that text message was a scam, and the person you talked to was not an Example Bank employee, it was a scammer.

Because you have no cash in your checking account, your automated mortgage payment bounces, and your debit charges incur overdraft fees. After spending hours on the phone with several real (this time) Example Bank representatives, you manage to get your stolen money back. The bank will not, however, refund $120 in overdraft and returned check fees, nor will it remove the late payment mark from your credit report because "that's our policy."

Thinking back on it all, you ask yourself: "How did this happen?" The answer is in the form of a chain of events that started on Facebook:

1. You clicked Like on the official Gold's Gym and OrangeTheory pages, and at some point made a Facebook post that said you'd like to get back to the gym, but you can't afford it right now.

2. You clicked Like on Netflix because before you cancelled the service, you wanted to know about new exclusive shows when they launched.

3. You clicked Like on Dell because hey, you lowercase-L *like* Dell computers!

4. You clicked Like on Fender Guitars because you've always wanted one.

5. You clicked Like on Example Bank to get the credit card deal.

6. You posted a public photo to Instagram, identifying yourself as an Example Bank customer who has a Visa card.

7. You recently searched Google for "gym membership deals," "used Fender guitars," and "PC upgrades."

8. Facebook and Google each profiled you based on your public Internet activity, and "shared" this information with their "partners," who then used the advertising platforms on Google and Facebook to target your interests.

9. Example Bank "shared" the fact that you have a new credit card, are receptive to email communication, and any other potentially valuable information about you that they could, with their "partners," who then used it in ads, spam, and junk mail that was specifically tailored to your interests, location, and demographics.

10. A thief searched Instagram for people who posted "I heart Example Bank" selfies, then searched Google for their names. The top result was the resume you posted to Indeed.com last year, which gave the thief your full name, address, and mobile phone number. The thief then sent you a phishing (this term is defined in Chapter 3) text message, knowing that you have an Example Bank Visa card and probably a checking or savings account, too.

As you can see, even something as seemingly harmless as clicking "Like Us On Facebook" can start a chain of events that will lead to overconsumption, identity theft, and financial ruin. The thief didn't need elite hacking skills or special tools; everything required for this theft was available to anyone who has a phone and access to the public Internet. Even if you hadn't fallen for the phishing scam, you still ended up with $4000 of extremely expensive debt that you would not have accumulated if you hadn't painted a target on yourself for marketers armed with knowledge of your interests and credit availability. Those credit-based "deals" that you accepted will now cost you substantially more money than if you'd paid the full price in cash.

Resist the Urge to Share Information

Trickery often involves something fun and interesting. If you've been on social media long enough, then you've almost certainly seen someone share a post that says something like: "To get your 'porn name,' add your first pet's name to the name of the street you grew up on," followed by hundreds of replies from people who freely shared that information. Do those two pieces of information sound familiar – your first pet's name and the name of the street you grew up on? That's right – those are common two-factor authentication security questions! Now consider how many people have revealed *two* possible answers to their security questions in a public Facebook post just because they thought it was funny to share their "porn name." (This is why I say that "secret questions" are a very poor MFA method; later in this chapter, I explain how to make "secret questions" stronger by using dummy information.)

If you participated in one of the those "porn name" social media posts (or anything similar), go find and delete your response right now. In the future, don't participate or share anything that asks you for any information about yourself, no matter how funny, harmless, obvious, or non-secret it may seem.

Good news is another gold mine for thieves and marketers. If you must share some good news, do it after the fact. Don't reveal things like this ahead of time:

- When and where you'll be travelling
- Jobs you're applying for, and job offers you've received
- Closing on a new house
- Colleges you are applying to
- Any financial information of any kind

After you've gone on the amazing 3-week vacation, or accepted the new job, or closed on the new house, then you can share the good news – at that point, thieves cannot target you as easily.

Case Study: Timing is Everything

Yes, even the fact that you'll soon be closing on a new house can be enough information for thieves to successfully scam you. In 2021, Tampa-area independent filmmaker couple Shane Brady and Emily Zercher were conned out of a $20,000 mortgage downpayment by clever thieves.[29]

When you're purchasing real estate it's normal and expected to give a large sum of money to a title company to hold in escrow until the closing documents are signed, so it didn't seem unusual at all when the couple received an email asking to wire their downpayment money to the title company that they'd been working with. According to Brady: "Everything [in the email] looked identical. The only difference was there was an employee named Sarah who had been spelling her name with an H and this was duplicated as Sara without an H."

They knew they'd been scammed when, after wiring their escrow money, the real title company called and asked for it. As of the publication of this book, the thief has not been caught. The couple says that they have no idea who the thief was, or how he or she knew how and exactly when to send them a request for a wire transfer that appeared to be from the correct title company. This was too precisely targeted to have been a random phishing attempt; that leaves a few reasonable possibilities:

1. Someone involved in the transaction (Realtor, title company employee, inspector, or an employee of the mortgage lender) either was the thief, or revealed the relevant details – knowingly or not – to the thief.

2. The thief thoroughly researched escrow scams, then closely watched public records and data sources (such as Zillow, Redfin, and MLS) for a pending offer, then used social engineering tactics (this practice is covered in Chapter 3) to discover the title company involved in the transaction, then crafted a legitimate-looking email to scam Brady and Zercher during the exact timeframe when they were expecting to make an escrow payment.

3. Either Brady or Zercher (or a close friend or family member) revealed on social media that they were closing on a new house,

[29] *https://www.tampabay.com/life-culture/arts/movies/2023/10/17/tampa-bay-film-shane-brady-aaron-moorhead-loki/*

and a thief saw that and knew how to use public data sources and social engineering tactics to intercept the downpayment as explained in scenario #2.

If Shane Brady and Emily Zercher had had the benefit of my advice at the time, they'd have known to distrust by default all requests for payment, to never give out any information unless they initiated contact, to be skeptical of the email that appeared to be from the title company, and to only communicate with the title agency through official channels.

This isn't just applicable to house purchases. If a thief knows your cell phone number, and that you are a Verizon customer, he or she can send you a phishing text message claiming that there's a problem with your payment method and that your service will be discontinued if you don't call to resolve the issue immediately. Ditto with car, mortgage, federal tax, and credit card payments. If a thief knows that you've just ordered something from Amazon or AliExpress, he or she is in a good position to execute the exact same scam.

Migrate From "Free" Services to Privacy-Focused Alternatives

Most people use "free" email, contact management, and file storage services from companies like Google, Apple, Yahoo, and Microsoft. Some people use the email and storage services included with their ISP, though increasingly ISPs have either discontinued their user services, or outsourced them to one of the aforementioned "free" providers.

I put "free" in quotes here because while these services may be free of charge, the companies that provide them are secretly earning or subtly extracting money from you in other ways; in other words, they are only *nominally* free.

Stop and think about it: How can companies such as Google, Microsoft, Yahoo, and Apple afford to provide unlimited email service with many gigabytes of storage to billions of people who aren't paying for it? There are only four reasonable scenarios:

1. **It's an upsell to a more fully-featured and privacy-focused "premium" or "professional" level of service.** Dropbox, for instance, can offer a "free" storage account with a frustratingly

small amount of storage and limited features because it's more or less the demo version of the paid subscription service. This scheme is not inherently dangerous to your privacy, but that doesn't mean it's inherently safe, either; it all depends on the company.

2. **It's a value-add incentive for buying expensive hardware.** Apple can afford to offer "free" services because the costs are offset by revenue from iPhone, iPad, and Mac sales, and from Apple Care subscriptions. This is not inherently dangerous to your privacy (depending on the company's policies and practices), but it's not good for you, either, because it eventually leads to an unethical practice that Apple is notorious for: **vendor lock-in**, where users or customers are prevented from easily switching to a competing device, service, or platform.[30] Apple does not make apps for non-Apple devices (with the occasional exception of some subscription media services such as Apple TV), so it's impossible to continue using Apple-based user services on other devices. Therefore if you really want to move off of the Apple platform, you must perform laborious manual processes to transfer all of your email, contacts, stored files, photos, secrets, and documents to other services; this is difficult by design.

3. **It's a method of collecting personal data and delivering targeted advertising.** "Free" services expose varying amounts of personal data to their host companies. If you haven't figured it out by now, I'll spell it out in plain English: the personal data that companies collect about you is worth a lot of money to them, and ultimately that money will come from you in the form of profits from purchases that you would not have otherwise made, or by manipulating you into making decisions that financially benefit a specific "partner" company, political organization, or foreign government that has paid for the opportunity to influence you.

4. **Some combination of the above.** Google uses its "free" user services as an information-collection scheme, a method of delivering targeted advertising, and a way to upsell its "premium" version of its "free" services.

---

[30] *https://www.theverge.com/2024/3/21/24107669/doj-v-apple-apple-watch-messaging-digital-wallets-lock-in*

If you want to protect your privacy and reduce the destructive influence of marketing campaigns, you'll have to pay for the services you use. My recommendations for privacy-centric digital services are in the subsections below.

Email

The most widely-used email services (as of this writing) are all "free:" Gmail, Apple Mail, Yahoo Mail, and Outlook (formerly known as Hotmail)[31], and they are provided by Alphabet (Google's parent company), Apple, Apollo Global Management (a private equity firm that owns 90% of Yahoo as of the publication of this book), and Microsoft, respectively. Among these companies, Apple is the least anti-privacy under Tim Cook's leadership, but that can change at the CEO's whim. What was important to Steve Jobs and Tim Cook will probably be of little concern to Apple's future CEOs. Google's founders, for instance, made "don't be evil" into the company motto[32], but after Google restructured itself into Alphabet, Inc. in 2015, that phrase was removed from its official corporate philosophy under new CEO Sundar Pichai.[33] Your digital security and privacy should never be subject to the decisions of corporate executives; rather, the companies you do business with should be fundamentally unable to ever use or even access the personal and private user information entrusted to them.

If you're using a "free" email service, I implore you to switch to a privacy-first service. It will cost a small amount of money because all services have costs, and there are no ads or data collection schemes to offset them. I'm concerned that this topic might be a hard sell for many readers, so I want you to consider these questions:

1. What would happen to you if you permanently lost access to your main email account?

2. What would happen to you if a thief were able to intercept all of your email for a month?

---

31 https://mailchimp.com/resources/most-used-email-service-providers/

32 https://web.archive.org/web/20050204181615/http://investor.google.com/conduct.html

33 https://www.searchenginejournal.com/google-dont-be-evil/254019/

3. How would you feel if your email service provider collected data about you based on the content of your emails?
4. How could you be manipulated if someone were able to read your emails?
5. What would happen in your life if your entire email archive were made public?

In the modern era, email is not just a method of communication; it also serves as a form of individual identification. For instance, email addresses are often used for/as:

- Usernames for sites and services
- Delivery of two-factor authentication codes
- Verification of identity when registering a new account
- The sole contact method for forums and sites such as Reddit
- Official association with an organization (via its domain name)

Consider the kind of information that might be stored in your email account:

- Financial details
- Health information
- Login credentials
- Secrets, confessions, and other private communication that could lead to extortion, job loss, or divorce
- Redemption codes for gift cards or store credit

Considering all of that, hopefully you agree that it makes sense to use a maximally-secure email service that has strong MFA and uses TLS to encrypt data in transit. But what about privacy? Google's Gmail service, for instance, is reasonably secure from intrusion if you enable strong MFA in your Google account; and Microsoft's Outlook.com email service is equally secure (if you configure it properly), has many useful features, and is free with an annual Microsoft Office subscription. These are not (as of

this writing) zero-knowledge services, however, and therefore the companies that operate them have the ability to access all of the data you store with them; they cannot be trusted to avoid collecting data about you through your email, or to keep your data safe from thieves and rogue employees. In fact, Google has already been caught spying on Gmail users[34] to provide better targeting for contextual ads (though it claims it stopped doing that in 2017[35]). Here's the user data it helps itself to, according to the privacy label it was forced to publish in order to offer its apps in the Apple App Store:

- Email address
- Name
- Your stored contact information
- Location
- Purchase history
- Anything and everything in your email and SMS text messages
- Photos and videos
- ID numbers for your devices
- Anything included in a crash report if a software bug causes the app to stop working

"Free" email services also allow senders to include hidden tracking code in email messages, which tells the sender your location (when you opened it), how long you viewed it (or had it open), the date and time you opened it, and whether you clicked on any links in it. Based on that data, marketers will adjust their strategy to be more effective at manipulating you into making the choices that benefit them at your expense.

---

[34] https://www.theguardian.com/technology/2021/may/09/how-private-is-your-gmail-and-should-you-switch

[35] https://money.cnn.com/2017/06/23/technology/business/google-ad-scanning-email-stop/index.html

Proton Mail

https://proton.me

Proton Mail is an email service developed by Swiss scientists who wanted to create a better Internet designed around user privacy, security, and digital freedom. It's zero-knowledge, end-to-end encrypted, and supports strong MFA methods.

Unlike most companies, Proton exists – in the words of its founders – "to serve the world [by] putting people before profits." Since its inception as a crowdfunding project in 2014, Proton AG has grown into one of the world's most prominent and active advocates for privacy and freedom online. As of the publication of this book, Proton has added several other products to its service:

- **Proton Calendar:** calendar / reminder / appointment management
- **Proton Drive:** cloud file storage
- **Proton VPN:** a no-log virtual private network that can weed-out trackers, ads, and malware before they reach your devices
- **Proton Pass:** a secrets-management system that also includes an email forwarding option so that you can hide your email address from websites that require it, and a 2FA authentication app

I highly recommend the entire Proton service suite; it has every tool you need to protect your privacy and enhance your digital security. The standard level of service is $3.99 per month (as of this writing) and includes all of the Proton products. If you need more storage or a faster VPN, you can upgrade to the Unlimited plan for $9.99. If you only want email, Proton does offer a "free" version of Proton Mail that is safe to use. This is free of charge because it has limited storage resources and is therefore an upsell to Proton's paid service levels; all of your email is still end-to-end encrypted, and the company does not collect or share customer information.

StartMail

https://www.startmail.com

StartMail is much like Proton Mail: it began in almost the same place (Netherlands) at almost the same time (2013), and has all of the same core features: zero-knowledge, end-to-end encryption, support for strong MFA methods, and email aliasing to protect your email address from being shared without your permission. It's slightly cheaper than Proton Mail, but as of this writing it's strictly an email service – no file storage, calendar, VPN, or secrets management system.

Email Masking

If you absolutely won't switch from your "free" email provider, then you can still enhance your privacy and security by using a service that obscures your true email address. Here are two I recommend:

- **DuckDuckGo Email Protection:** https://duckduckgo.com/email/
- **Firefox Relay:** https://relay.firefox.com/ (also offers phone number masking)

Email masking services provide unique email addresses upon request, then securely and anonymously receive, filter, and forward email to your primary email account. Spam, viruses, and tracking code are typically removed in the process, and you can manage your single-use email addresses through the provider's website.

If you don't want to go to the expense or trouble of subscribing to one of these services, you can create your own rudimentary single-use emails with the + symbol. Whenever you have to give your email address to a company, you can append an identifier to it that will enable you to track and filter the sender. Just add a plus sign to the username portion of your email address, then an identifier, then the `@` and your normal email domain name. For example if your email address is `stephan@example.com`, and you are giving your email address to a Ford dealership to be notified when the next delivery of Mustang cars arrives, you might use this email address instead: `stephan+ford@example.com`. Email servers ignore the plus and the

identifier, so all email sent to this address will go to your inbox as usual. However, if the Ford dealership starts spamming you, you can add a filter to your email program to send all mail sent to that specific address to the spam folder. If you start getting email sent to that special address from anyone other than the Ford dealership, then you'll know who sold your contact information.

Unfortunately some marketers are wise to the + email masking trick, and have implemented rules in their sign-up forms that prohibit using the + symbol in an email address field. I advise you to avoid any such sites or services whenever possible. If you aren't able to avoid them, and you don't want to sign up for an email masking service, you should consider setting up a secondary email account – perhaps with a "free" provider such as Gmail or Yahoo – that you can use specifically for this purpose.

Sometimes blocking the + symbol in signup forms isn't the result of greedy marketing practices, but of ham-handed security measures. Hackers often attempt to break into Web-based services by using a technique called **cross-site scripting** (**XSS** for short), in which the attacker uses special characters (usually punctuation marks and the symbols you get by holding the Shift key and pressing a number key on your keyboard) in text fields to trick the software into retrieving restricted information from an internal database. Talented software engineers know how to pare down the list of allowable text characters so that only the actually dangerous ones are prohibited, but many of the people who write much of the world's Web and app software will simply exclude all special characters except for the @ because it's quicker and easier.

Web Browsers

The Web browser world is – and has always been – glacially shifting toward one preferred option after another. As of the publication of this book, the Chrome browser (developed by Alphabet) has the title of most-used Web browser at over 60% of all legitimate human webpage visits (excluding visits or downloads from automated programs), followed distantly by Apple's Safari, Microsoft's Edge, and Mozilla's Firefox.[36] If you consider the fact that Edge, Opera, Silk, Brave, and Vivaldi all use Chrome's Blink

[36] *https://en.wikipedia.org/wiki/Usage_share_of_web_browsers*

rendering engine, then Chrome-based browsers account for more than 70% of human Web activity.

The "browser wars" of antiquity were focused on which browsers worked best with certain sites or apps. Some websites only worked properly in Microsoft Internet Explorer; others, only in Netscape Navigator (both of which have long been discontinued as of the publication of this book). Fortunately the dark days of webpages appearing vastly differently depending on which browser you use are over, so there is rarely a need to use more than one. Unfortunately it's impossible to completely remove the default Web browsers that device manufacturers and operating system developers foist on their users, so more than two decades after the end of the "browser wars" we're all still forced to download, install, and switch to a different Web browser – this time to protect our privacy.

In terms of safeguarding users from security vulnerabilities and privacy violations, none of the major Web browsers is inherently terrible; unfortunately most of them aren't great, either. Chrome and Edge push users into sharing data with advertisers and creating accounts with Google and Microsoft, respectively; and Safari is entirely controlled by Apple.

Fortunately there are some excellent alternatives that are either developed by open-source software projects or small companies that are fundamentally committed to maximum privacy protection for users:

Firefox

https://www.mozilla.org/en-US/firefox/

If you consider the fact that Firefox was originally developed from the open source code from the once-dominant Netscape Navigator Web browser, that makes it the oldest continuously-developed graphical Web browser in the world.

Firefox is developed by the Mozilla Corporation, which is owned by the Mozilla Foundation; both organizations have a long history of supporting and advocating technologies that help people protect their digital privacy and security. One of my favorite Mozilla Foundation products is the *Privacy Not Included* blog, where researchers publish their analysis of the privacy and security risks of buying or using a wide variety of consumer products:

https://foundation.mozilla.org/en/privacynotincluded/

Over the past decade Firefox has grown beyond its origin as an extensible, barebones Web browser. It now includes the following extra services:

- Password management
- Pocket: a searchable archive of bookmarked articles
- Mozilla VPN
- Firefox Relay: email and phone number masking
- Firefox Monitor: data breach search and monitoring
- Integrated blocking of third-party cookies, tracking scripts, and video autoplay

You can also add extensions that will block ads, prevent pop-up windows from appearing, and isolate all Facebook tracking to an isolated browser tab.

If you want extra privacy protection, you can easily open a Private Window in Firefox that will not retain any session data, and will not allow any webpages to communicate with other browser tabs or windows.

One thing I don't like about Firefox is that Google is its default search engine; and as I'll explain in the "Why Web Browsers Are 'Free'" section later in this chapter, Google collects and uses a lot of user data. Fortunately you can easily change this setting to a non-invasive search engine such as Brave or DuckDuckGo (both of which are covered later in this chapter).

Brave

https://brave.com

The Brave browser was designed from the beginning to protect user privacy and security above all else. In the words of Brave's founders: "The internet is a sea of ads, hackers, and echo chambers. Big Tech makes huge profits off our data, and tells us what's true and what's not. Brave is fighting back. Brave is on a mission to protect your privacy online."

Brave uses the same open source Chromium framework that underpins most other Web browsers. What makes it unique is its Shields function, which zealously blocks all trackers and invasive ads by default. If a webpage doesn't work correctly because one of its elements is blocked due to a privacy risk, you can choose to reduce the level of resource blocking, or completely disable Shields temporarily for a specific site. Brave also has integrated support for **TOR** (**The Onion Router**, a network technology that encrypts all traffic and protects the privacy of website owners and visitors), and – like Firefox – you can easily open a Private Browsing window that retains no session data and cannot interact with other browser tabs.

Also similar to Firefox, Brave Software produces much more than just a browser:

- **Brave Search:** a Web search engine
- **Brave Talk:** a privacy-focused video conferencing service similar to Zoom
- **Brave Firewall + VPN**
- **Brave Wallet:** a cryptocurrency wallet
- **Brave Playlist:** an audio / video playlist-creation app
- **Brave News:** a newsfeed for blank browser tabs
- **Leo AI:** a large language model artificial intelligence engine similar to ChatGPT

Vivaldi

https://vivaldi.com

Vivaldi is similar to Brave in that its design gives power to the user instead of the developer, but Vivaldi goes much further with this philosophy than any other Web browser. You can customize nearly every aspect of Vivaldi's interface and behavior, much moreso than Firefox or Brave. If you're a more technically-inclined user who enjoys fine-grained configuration, Vivaldi may be the perfect solution for you; on the other hand if you just want a browser that works without having to mess with it too much, then

Firefox or Brave are probably better options. There's no harm in installing Vivaldi alongside Brave, Firefox, or any other browsers, so go ahead and try it out.

Why Web Browsers Are "Free"

Earlier in this section I advised you to consider why valuable software and services don't cost money to use. The three primary scenarios I presented were: to upsell to a paid product, as a value-add for buying hardware or other products, and as an advertising platform and a user data collection tool. At various points in history, Web browsers have fit into all three of those categories. Today, however, the companies that produce the most popular Web browsers all have one primary goal: *to capture search revenue.*

Search engines pay a lot of money to the companies that develop and distribute popular Web browsers for the privilege of being the default search engine when users type search queries into the URL field. During an antitrust lawsuit in 2023, it was revealed that in 2021 Alphabet paid more than $26 billion to Apple, Mozilla (Firefox), Samsung, and various wireless service providers and mobile device manufacturers to guarantee that Google would be the default search engine in their products – that's more than 15% of the company's $165 billion in total revenue that year.[37] Other search engines such as Yahoo, Baidu, and DuckDuckGo have also paid for the right to be the default in certain products or regions.

Aside from search revenue, Firefox's parent company also sells other subscription services that focus on enhancing user security and privacy, such as its VPN and email masking products, and the premium edition of its free online article archive utility (Pocket).

Brave Software sells a subscription VPN service similar to Firefox, and a premium version of its Brave Talk video conferencing service. Brave also makes money by selling physical merchandise, selling ads (without invasive tracking or data collection) in its default new browser tab and newsfeed screens, through affiliate links to online retailers, and through text ads integrated into its Brave search engine.[38]

---

[37] *https://www.theverge.com/2023/10/27/23934961/google-antitrust-trial-defaults-search-deal-26-3-billion*

[38] *https://productmint.com/brave-business-model-how-does-brave-make-money/*

Web-based businesses may also pay browser companies to include bookmarks to their sites. When you install Vivaldi, for instance, links to Booking.com, eBay, and other sites are automatically added to your bookmarks menu (you can remove them manually). Vivaldi also generates revenue from its Direct Match feature, which includes links to certain relevant sites in the autocomplete list when users type search queries or URLs into the URL field.

So that's how Firefox, Brave, Vivaldi, Opera, and other "free" browsers can afford to pay developers and other employees without collecting, using, and selling your personal data. Similarly, Alphabet's effort to develop and distribute the Chrome browser is simply a way to save money; it does not need to pay itself to make Google the default search engine in its own Web browser. Likewise Microsoft makes its Bing search engine the default in its Edge browser, which is preinstalled (and can't be uninstalled) and made the default (unless you manually change it) on all Windows devices.

Search Engines

Google legitimately earned its place as the world's top search engine through its superior methods of reading, categorizing, and archiving websites, and delivering fast and accurate search results through a minimalist interface. It eventually became profitable by collecting data about searchers (and later, users of other Google services) and showing them targeted ads in search results, apps, and on websites.

For the first two decades of the 21st century, no search engine was able to legitimately compete with Google, but that's no longer true. It used to be farcical to complain about the quality of Google Search, but over the past several years many journalists and power users have openly criticized its results as irrelevant and spammy, its interface as clogged with ads and bloated with unwanted features, and its data collection and sharing practices as invasive and manipulative. *The Atlantic's* Charlie Warzel succinctly described Google's decline in a 2023 article on the topic:[39]

[39] *https://www.theatlantic.com/technology/archive/2023/09/google-search-size-usefulness-decline/675409/*

> *Unlike its streamlined, efficient former self, Google Search is now bloated and overmonetized. It's harder now to find answers that feel authoritative or uncompromised; a search for healthy toddler snacks is overloaded with sponsored product placement, prompts to engage with "more questions" (How do you fill a hungry toddler? "Meat and Seafood. Bring on the meat!"), and endless, keyword-engorged content. Using Google once felt like magic, and now it's more like rifling through junk mail, dodging scams and generic mailers.*

Even if you aren't concerned about your privacy, it probably benefits you to start using a better search engine.

If you own Android-based mobile devices, it's impossible to completely dodge Google (on the other hand, your only alternative is another huge corporation: Apple). However, you can easily replace Google Search with alternatives that deliver good search results – better than Google, often – without collecting data about you and then crapflooding your search results with a multitude of targeted ads based on it, and "features" that are neither useful nor wanted.

Both of the Web search engines explained below are safe to explore. Try them out and see if you prefer one over the other, then make it the default search engine in your Web browser(s). If your mobile devices have a Google Search widget on their home screens, then you can replace it with an equivalent app and widget from DuckDuckGo or Brave.

DuckDuckGo

https://www.duckduckgo.com

DuckDuckGo describes itself as: "the independent Internet privacy company for anyone who's tired of being tracked online and wants an easy solution." It began as an alternative to Google Search, but – as I mentioned earlier in this chapter – recently it has expanded to other privacy-focused

services that help you use the Internet without allowing corporations to collect information about you without your knowledge or consent.

DuckDuckGo reminds me very much of the Google of old: a simple interface, plain Web search results (with tabs to view vertical search results such as images, news, or video), and a few unobtrusive text ads that don't target you based on your personal data or use third-party cookies to follow you around the Internet.

Building a Web search index in the modern era is a Herculean task. Most search engines have the advantage of a head-start from a bygone era when there were only about a million Web pages, most of them static (meaning they don't change without human intervention); today there are more than a billion pages, and many of them change dynamically and rapidly via automation.[40] DuckDuckGo is gradually building its own search index through traditional automated Web crawling, but it also incorporates structured data from large public databases such as Wikipedia and Sportradar.[41] Wherever there are information gaps, DuckDuckGo relies on search data from Microsoft's Bing search index (though it does not share private information with Microsoft).

Most of the time DuckDuckGo's search results are identical to or comparable with Google's even though they have different methods of finding and cataloguing information, but sometimes they differ. Sometimes that difference is good – DuckDuckGo is better – and sometimes it isn't. Before running back to Google when your search results don't instantly yield the answers you're looking for without refining the query, I suggest trying Brave Search (introduced below) first.

Brave Search

https://search.brave.com

As part of its expansion of privacy-focused user services beyond its Web browser, Brave Software has developed a search engine similar in ethos and accuracy to DuckDuckGo. Ironically DuckDuckGo is also in the process of developing a Web browser similar to Brave. As far as I know, the two companies aren't directly competing with each other; rather, they

[40] *https://www.netcraft.com/blog/june-2023-web-server-survey/*
[41] *https://duckduckgo.com/duckduckgo-help-pages/results/sources/*

have the same goal of helping people use the Internet without sacrificing privacy or security.

Brave Search differs from DuckDuckGo in that it does not rely on Bing for extra results (though it used to, prior to 2023).[42] Brave has built its own private search index that it continually refines through traditional automated Web crawling, anonymous browsing data contributed by Brave Browser users who have opted into its Web Discovery Project, and direct feedback from Brave Search users.[43]

Whenever Brave Search delivers substandard results, users are given the option of enabling the Google Fallback Mixing function, which reruns your Brave Search query in Google without passing any personally-identifying data along with it.[44]

Messaging

There are two kinds of text messaging paradigms: traditional mobile phone-based **SMS (Short Message Service)** and **MMS (Multimedia Message Service)** text messages that are handled by a wireless service provider, and cross-platform instant message or chat services that communicate over any Internet connection.

SMS text messaging is a very old communication platform that has no support for modern media formats, and is about as secure as passing a note in 6th-grade study hall. Your wireless carrier and the company that publishes the messaging app can read and record every SMS text message you send, and messages can easily be intercepted by using wireless hacking tools. MMS was built on top of SMS, and enables sending some media files, but it's still fundamentally insecure. For many years big tech companies and cellular service providers have been trying to completely replace SMS / MMS with something more secure and capable of transmitting more than just plain text and images. This effort culminated in the **RCS (Rich Communication Services)** messaging framework which is end-to-end encrypted, allows a variety of rich media formats to be transferred, and natively supports extra features like read receipts and real-time typing notifications. As of 2025 RCS has been implemented in

---

42 https://brave.com/search-independence/
43 https://support.brave.com/hc/en-us/articles/4409406835469-What-is-the-Web-Discovery-Project-
44 https://search.brave.com/help/google-fallback

most cellular networks, and is used by default in the Google Messages, Apple Messages, and Verizon Messages+ apps. If you send a message to a recipient who is not on an RCS-capable network or isn't using an RCS-compatible messaging app, then your messaging app will fallback to SMS / MMS.

While text messages are traditionally the exclusive domain of mobile devices, instant messaging or chat services allow you to send and receive multimedia messages across multiple platforms (PC, mobile, tablet, etc.) over any Internet connection. As of this writing, the most popular instant messaging services are: Facebook Messenger, Snapchat, Whatsapp, and WeChat, all of which have terrible privacy records and practices.[45][46] Fortunately there are alternatives. I have two recommendations for instant messaging services that I have complete confidence in (explained in the following subsections), but I don't want to rule out smaller projects that I'm not aware of, so I'll provide you with a list of necessary features that a secure and private chat / instant messaging app must have:

- Strong end-to-end encryption
- Strong multi-factor authentication
- Doesn't keep messages in a device's permanent storage
- Doesn't monitor and record user activity
- Messages can be set to self-delete
- Developed from open-source code

And some nice-to-have features that will help you maintain your security and privacy:

- Multi-mode communication (you can send text messages as well as photos, GIFs, and other files)
- Message and contact synchronization across multiple devices

The biggest hurdle to changing instant messaging platforms is your friends and family, who are probably all on an insecure and privacy-averse

[45] *https://www.comparitech.com/blog/vpn-privacy/is-snapchat-encrypted/*
[46] *https://www.bbc.com/news/technology-59348921*

platform like Facebook. I suggest that you ask them to switch to one of the services I recommend below. At worst, they have one more app on their mobile phones, and may have to send group messages to you separately. Realistically most people probably aren't going to switch no matter how persuasive you are, but it's still worth a try. If you aren't able to completely migrate off of insecure instant message services, at least be mindful that your messages are not private.

Signal

https://www.signal.org

Signal is a zero-knowledge, end-to-end encrypted app that provides instant messaging and voice call services. Originally it also supported SMS text messaging, but that feature has been discontinued for security reasons. It's based on open-source software and open standards, and it's owned and managed by a non-profit company that, by rule, cannot be acquired by a for-profit corporation. It is "free" because it is funded through grants and donations. The company does not collect or sell user data, and is therefore fundamentally unable to comply with warrants that give law enforcement access to a user's messages, contacts, or location data.

Threema

https://threema.ch

One of the biggest perks of Threema is that you don't need a phone number or email address to sign up. You get a unique Threema ID key when you launch the app, and you can add other users with a scannable QR code. All forms of messaging (text, voice, picture, video) are encrypted on Threema. You can also share files through the app and generate polls in group conversations. Threema is based in Switzerland, which has a high national and cultural standard for user and customer privacy, so the company is legally unable to collect or use your information. This app is not "free;" it costs $3.

File Backup and Cloud Storage

If you use a cloud storage provider or backup service such as Microsoft OneDrive, Google Drive, or Adobe Cloud… well, by this point in the

chapter I hope you can guess what my advice will be. Here are some safer and more secure alternatives:

- **Proton Drive:** https://proton.me (this is part of the Proton suite that I've covered in other parts of this chapter)
- **Box.com:** https://www.box.com
- **Tresorit:** https://www.tresorit.com

Change Your Mailing Address to a Post Office Box

Your home address is a valuable piece of information for both marketers and thieves. Unfortunately it's also public information available through various sources such as court records, real estate transactions, voter registration, driver's license data, donor databases, and credit reports – and, of course, whenever and wherever you've voluntarily published or shared your home address online or with a corporation.

As I explain in detail in Chapter 6, removing your personal information from the Internet is a long-term process, and it isn't possible to completely erase all of it – even after you're dead. That doesn't mean it isn't worth the effort; every meaningful action you take to protect your privacy has an immeasurable long-term benefit. No matter which piece of publicly-viewable personal data you're trying to remediate, the first step is always the same: start using a safer alternative from this point forward. For your home address, this means obtaining a separate mailing address that you will henceforth use for all official correspondence.

The cheapest and easiest alternative mailing address solution is a Post Office box (PO box) with one of your local Post Office branches. You can get a PO box at any Post Office; it does not need to be in the same ZIP code as your home address. The small- or medium-sized boxes will be fine for ordinary residential mail. If you receive anything at your PO box that requires a signature or won't fit in the box, you'll be able to sign for it or pick it up at a locker or at the counter. Some Post Offices do not accept package deliveries from other carriers (UPS, FedEx, DHL, Amazon) to PO boxes directly, but many branches do offer a package-receiving service (with a slightly different delivery address) as an add-on. Rather than have packages sent to your PO box, you'd have them sent to the Post Office branch along with special codes that correspond to your box. For instance,

if you had a PO box at the main Post Office branch in Orlando, FL (which does offer a package-receiving service), your PO box address might be:

> John Doe
> PO Box 12345
> Orlando, FL 32862-2345

But to receive packages, you would provide this address instead:

> John Doe
> 10401 Post Office Blvd W FL 3 #12345
> ORLANDO, FL 32862-8543

The only downside to a PO box (other than cost) is that you'll have to go pick up your mail in person, usually during the hours that the Post Office counter is staffed. However, most large metropolitan areas have at least one branch that offers 24-hour access to PO boxes; be sure to inquire about this before you sign up for one.

Apart from the US Postal Service, there are other mail- and package-receiving services that might offer lower prices or more features (such as a mailing address that doesn't look like a PO box) in your local area. I trust you can find and evaluate those on your own by using a search engine.

Once you have your new mailing address, update your contact information for every service you use. Usually when you change your mailing address with your bank or credit card company, that will also cause it to become a valid billing address for all credit and debit purchases (but you should check to make sure there aren't any extra steps; some banks may require you to explicitly define an auxiliary address for online purchases). This means that whenever you pay for something online and are required to provide a "billing address," you should be able to use your PO box. If you must provide a separate shipping address, you can either provide your package-receiving address (if you chose to add that service to your PO box) or your home address. Obviously it's better to avoid using your home address at all, but sometimes it's unavoidable, such as when you're having an appliance delivered or a home-based service installed (such as cable television or Internet services).

There are some situations where you're legally required to provide your current home address. All financial institutions (including banks, credit unions, brokerages, lending agencies, and cryptocurrency exchanges in the US) are required by Federal law to collect and verify four pieces of personal

information about every account-holder: full name, date of birth, home address (this must be a valid residential address; it cannot be a PO box), and an ID number from a state- or government-issued ID (usually a driver's license, passport, or military ID).[47] Officially this practice is known as **know your customer** (or **KYC** for short). Your KYC information must be re-validated periodically, and it, plus all of your transaction data, must be kept for at least five years, even if you close your account; this is required by Federal law for **anti-money laundering (AML)** and **counter-terrorism financing (CTF)** purposes.

Aside from that, obviously your utility service providers need to know where you live. There may be other circumstances where you are legally obligated to provide your home address; I leave it up to you to use your good judgement to determine when and where those circumstances are. But in general, from this point forward, whenever you're asked for your address, use your PO box instead of your home address. Gradually – and especially if you move to a new home – your PO box will replace your home address in many personal information databases, which will make you less vulnerable when those databases are stolen or breached.

Remove Personal Information From Your Domain Registration

Do you own one or more website domain names? If so, ensure that your home address and other personal contact information are not visible in the domain records. You can view or change those details through your domain registrar, but it's quicker to use the registration data lookup tool provided by **ICANN** (the non-profit **Internet Corporation for Assigned Names and Numbers** – the closest thing the Internet has to a central government):

https://lookup.icann.org

If you can see your name and contact information there, then so can the entire world. ICANN requires that there be a legitimate contact for technical, administrative, and spam issues relating to each domain. However, domain registrar companies are allowed to serve as the single point of contact for their customers, which enables you to remove your

[47] *https://www.investopedia.com/terms/k/knowyourclient.asp*

personal information from your domain metadata (I explain what metadata is and how to alter it in Chapter 8), and replace it with the public contact information for your domain registrar. This usually costs extra. If you're unable or unwilling to pay the extra domain anonymization fee, you can still update your domain records with safer (but still valid) alternatives: a masked email address and phone number, and a PO box for a mailing address.

Revoke Unnecessary Location Sharing

How many times have you been asked to share your location with a website or smartphone app? Hopefully your answer is: "Too many to count!" If not, then you may have given blanket permission to share location data at some point, and it is currently being collected and shared by default. Take some time to review the privacy settings in your Web browser, car (if it has built-in navigation or location tracking features), and all of your connected devices (smartphone, smart watch, earbuds, etc.). Ideally you should be asked for permission every time you share your location data, and location permission should be revoked immediately after you're done using the device / site / app / service, or after a set interval of time. This isn't just good for your privacy; it also prevents unnecessary battery drain on your mobile devices because location services use a lot of power, even when you're not actively using any apps.

A lot of location sharing requests are completely unnecessary and can be categorically rejected, such as on websites that have a "find a local store" search function. You can just as easily type in a city name or postal code. I took a moment to think about it, and couldn't come up with a good reason why a Web browser (or website) would ever need to know your exact GPS coordinates. Besides, in many cases your current location isn't the one you want search results, directions, or recommendations for.

You probably do want at least some smartphone apps to have access to your location sometimes, but a lot of the time it isn't clear why a smartphone app is even asking for location permissions. There's generally no harm in denying permission for an app; if you end up needing it, you can simply re-enable it through your device's permissions settings. The best option to choose is "Only this time," because the app will explicitly ask for permission to access your location data every time it wants to use

it. This is a little inconvenient sometimes, but inconvenience is often the price of both privacy and security.

It may seem Orwellian at first – companies being able to track and record your exact location – but you should set that aside for a moment and consider the potential benefits of device-specific location tracking. You may not want Ford to track where your truck goes… until it gets stolen, or you forget where you parked in a huge parking lot, or you're locked out because you lost your key fob, or you've been involved in a bad accident in an unfamiliar area and need emergency services. You may balk at enabling location sharing on your smartwatch… until you lose it, and discover that you cannot use the "find my watch" feature from your smartphone.

Is it worth it to you to enable always-on location sharing sometimes? Maybe it is! I'm not going to tell you you're wrong or unsafe; I just want you to understand what you're doing and why you're doing it, and to encourage you to be in control of the information you reveal. Just because an app asks for permission doesn't mean you have to grant it (or grant it permanently).

Total, comprehensive protection for every aspect of your privacy is not feasible under most circumstances. Even if you turn off location sharing on every device, and even if you use a stupidphone instead of a smartphone, it's still possible for law enforcement to track you based on things like cell tower triangulation, surveillance technologies with integrated face and voice recognition capabilities, credit card purchase history, and just plain-old asking your neighbors and co-workers for your whereabouts. You can't live in the modern world and hide from every person, security camera, microphone, or motion sensor. The point is not to disconnect from everything and try to be completely unfindable, though; it's to do what you reasonably can to prevent your location data and history from being used without your knowledge – especially for commercial purposes.

Use Dummy Information

Dishonesty is almost universally immoral. *Almost.* One valid exception to the rule is when a lie will protect you or your family from harm. It's up to you to decide if this reasoning can be extended to protecting your

information and data, but if you want to maximize your privacy and security, you should find a way to be comfortable with lying to corporations about some of your personal details.

I do understand that some readers of this book will demand to take a principled stand and refuse to participate in moral relativism. If that's your position, then you can skip down to the "security questions" paragraph later in this section. My opinion is that there is no honor in unnecessary martyrdom; it does not benefit you or your family to be self-destructive solely on principle. Psychopaths lie for amusement, but ordinary people lie when they are forced to defend themselves against a power imbalance. When someone forces an unfair ultimatum on you, or threatens to gatekeep you from accessing an important service, or in any way attempts to strongarm you into giving up personal information that he or she does not legitimately need and has no right to collect, then go ahead and give him or her dummy information. Beware the slippery slope; do not use false information to obtain credit, or in any kind of contract, and do not lie to law enforcement or while under oath – that will get you arrested.

Let's go back to the example of the dentist office assistant who wants to swipe or photocopy your driver's license before you can have any dental work done. If you refuse to provide your license, then the assistant might refuse to register you as a patient, but if you say that you *don't have* a driver's license or other ID with you, then you might be able to get past the gatekeeper. Refusing to provide your photo ID is a battle of wills with someone who has power over you; not having a photo ID to provide, however, makes it seem like you don't have a choice in the matter, and that may make the gatekeeper feel less inclined to bully you. The same is true with hospitals and office buildings that are generally open to the public, but have a security check-in. Perhaps they'll deny entry if you don't have photo ID, but clearly they do make exceptions in certain cases, most notably with minors. Occasionally this is something you can't get out of, such as when you're test-driving a car or touring an apartment that you're considering renting; in these instances, the best you can do is ensure that photos and photocopies are destroyed before you leave.

What about a "fake" photo ID? Non-government-issued photo IDs are not governed or regulated by law as far as my research shows. As long as you're not pretending to be someone else, providing false or fraudulent information, or attempting to gain access to a restricted area, you're free to create your own non-government-issued photo ID, and you may

present it in lieu of a driver's license when requested (though I wouldn't advise giving it to a cop, or in any other legal setting). Obviously you cannot create a fake driver's license, passport, or military ID, and though it's not technically illegal, it's probably not a good idea to create a fake student ID (and if you're falsely purporting to be a student at a real college, then that would be fraudulent and therefore illegal). Press passes are generally issued by publishers and are not regulated by any government or professional organization, but I don't recommend creating a press pass for yourself unless you intend to use it in the course of actual journalistic business. If you want to create an alternative photo ID for yourself, just print your name on a card-sized piece of paper alongside a headshot photo, and perhaps the words "Personal Photo Identification" at the top, and laminate it. Alternatively you could do what many Realtors have done for decades: add a professional headshot photo to your business cards, and use them for photo ID.

Don't accept the excuse that handing over your driver's license to be copied or scanned is "for your security." It isn't. It's actually dangerous to your security in a number of ways. You could have handed that clerk or secretary *anyone's* driver's license; how would they know it isn't yours? Likewise, what if someone steals your ID and uses it as their own? More importantly, an identity thief could easily make a fake driver's license with your name and photo on it, and no one short of law enforcement would have the tools and legal authority to legitimately validate it. Think about the past 10 times you've handed your driver's license to someone – to a dentist's office assistant, to a clerk or bartender to buy alcohol or other age-restricted products, to a bank teller to cash a check. Did any of those people even *attempt* to verify that your physical appearance matches the photo and description on your driver's license?

Also consider the companies that ask for part or all of your social security number for "security" or "identification" reasons. Verizon may need your SSN to pull your credit report when you apply for service, but it isn't legally allowed to record the number or keep the report, so what's the purpose of asking you for the last four digits of your SSN "for security purposes?" They have no way of knowing if those four digits are correct because they aren't supposed to have your SSN at all. Really this is just a request for a 4-digit PIN that you aren't likely to forget. In these situations, you're free to make up any number you want, as long as you securely keep track of it in your password management app.

"Security questions" (as a 2FA method) are another good opportunity to protect yourself by making something up. If you follow the rules, then they're a very poor method of two-factor authentication because the true answers are easily obtained. Consider these typical security questions:

- What is your mother's maiden name?
- What was the name of the street you grew up on?
- What is your father's middle name?
- What is your maternal grandmother's first name?
- What was the name of your first pet?
- In what year were you married?
- What was your high-school mascot?
- What is the name of a memorable place?
- Who was your first employer?
- What was the name of your first-grade teacher?

Are the answers to these questions even *remotely* considered secrets? Would you normally be wary of sharing *any* of this information, even with a friendly stranger? How much of it could be obtained from your Facebook page, or from a brief conversation with you or someone you're close to? Companies that use these kinds of security questions may as well ask "who is buried in Grant's tomb?" or "in what sport do the players wear tennis shoes?"

It benefits you to make up (and securely record) unique untrue answers to these kinds of security questions, and to use different answers for each site or service that requires them. This essentially makes your security question answers into secondary passwords, and in fact it would be a good idea to use your password manager to generate a secure password or passphrase to use for each security question. By using unique fake answers (and securely recording them), even if an attacker were to know every true answer to your security questions, he or she would not be able to use them to compromise your accounts.

Also consider the fact that many of these questions are irrelevant for some people. Perhaps your mother didn't change her last name, or your father is Spanish and has many "middle" names, or you never had a pet or owned a car. Even if you don't want to lie, you may have to make up an answer anyway, so you may as well increase your security by making them *all* up.

Protect the Vulnerable

Now that you've taken the necessary steps to protect the privacy and digital security of yourself, your family, and your business (if applicable), you should begin thinking about friends, neighbors, and extended family members who are at greater risk of having their private information used against them.[48]

We often expect that the elderly in general do not understand how to safely interact with technology, but they may also fall victim to old-fashioned scams such as door-to-door or in-home sales pitches, and requests for donations through regular mail. Scam phone calls are also a huge problem for people who've spent most of their lives inherently trusting that whomever is calling them is who they say they are, and that the call is important. You can't intercept every scam, but you certainly can educate an elderly loved-one on all of the concepts and practices that I explained in Chapter 1. If you only choose one thing to focus on, it should be: *always distrust all requests for payment.*

At the other end of the age spectrum, children are also easily manipulated, especially online. A child should never have unrestricted access to social media or any kind of instant messaging service – *especially* the privacy-focused ones I recommended earlier in this chapter. Let me be clear: as a parent, you absolutely should violate the digital privacy of your minor children in every way possible. Enable location tracking on their devices so that you know where they go, and closely monitor whom they communicate with, and what the nature of their text and email conversations are. Make it a rule that you must always know who your children are exchanging messages with – no exceptions! Having said that, don't go overboard. Kids talking to kids they know from school or the neighborhood about ordinary kid things isn't worthy of parental

[48] *https://www.theatlantic.com/ideas/archive/2023/07/elder-senior-citizen-scams-fraud-exploitation/674793/*

intervention. Kids talking to adults (even if they are or claim to be relatives, family friends, neighbors, teachers, police officers, politicians, celebrities, or clergy), or to "kids" whom your child has never met in person are causes for alarm. Predators can only be successful if they're allowed to communicate privately with children.

Maintain Vigilance

Even if you do everything right, you can still be a victim of identity fraud. Simply by knowing your name, home address, and bank account number, a thief can create and use a fake ID to withdraw cash from your account at a physical bank branch.[49] There is nothing you can do to prevent this, but if you are vigilant and act quickly, you can reverse or limit the damage.

When scenarios like this occur – including a thief stealing or duplicating your credit cards – your ability to recover stolen money or dispute fraudulent charges fades rapidly with time. If you catch these transactions when they happen (or very shortly after), then you can immediately call the bank and report it. Not only does this enable the bank to reverse recent charges and return stolen funds, it also prevents the thief from causing further damage.

Though it may be annoying, you should enable notifications by mobile app, SMS text message, or email whenever a charge is made to your credit cards, or any money is withdrawn from your bank accounts. If you're unwilling or unable to do this, then at very least log into your financial accounts via app or website every day or two, and review the list of recent transactions. Don't wait for the monthly statement to be mailed to you.

[49] *https://finance.yahoo.com/news/i-lost-11300-to-identity-fraud-what-i-learned-usual-safeguards-dont-work-220720605.html*

Chapter 3: The Scope, Hierarchy, and Value of Personal Data

Your personal data can be used to impersonate you for financial gain (identity theft), to steal directly from you (fraud, burglary, mugging, carjacking), to blackmail you, to subject you to vigilante justice (social media dragging / cancelling, SWATting), or to influence or alter your behavior in a number of ways. Before I get into what those ways are in Chapters 4 and 5, I want to clearly define what I mean when I say "personal data" or "personal information."

Personal information is any information that describes you, your property, or the services that you use. Within that, there are three primary categories: **public**, **private**, and **secret**. From now on, I encourage you to think about these three classifications before you share or reveal your personal information. This is very similar to the standard information security paradigm (also known as **infosec**) that governments and corporations use to classify all of their documents: public, confidential, secret, and top secret.

The words 'information' and 'data' are semantically similar and are often used interchangeably, but it's easier to understand the concepts in this book if you think of **data** as *recorded information.* When personal information

is written down on paper, stored electronically, or recorded as audio or video, it becomes **personal data.** The moment your personal data is created and stored by anyone other than you, you have permanently lost control over it.

Public Information

Public information is anything that any person could obtain about you through ordinary and unprivileged methods. For instance if you are walking down the street, then your appearance, location, and the direction you're travelling are all presently classified as public information, and this could be legally recorded in a variety of mediums. If your name, phone number, and address are publicly listed in a residential phone book, then that's all considered public data. If you buy a house, register a car, or are involved in litigation, the majority of the details will be recorded in public records that are, by law, available to the public (though some information can be redacted, for instance to protect the identity of a minor, or to prevent the release of important personal data such as your bank account number, credit card number, or social security number). There are many exceptions to these rules, but for the most part you should always assume that everything you do and say in public is the public's business, and that you are always being tracked and recorded unless you have a legally-recognized **reasonable expectation of privacy** (such as in a public restroom, lawyer's office, or medical exam room).

In the United States, citizens may not demand that their public words and actions be protected under most circumstances. There is a legal grey area around harassing, recording, or stalking private citizens; for your privacy to be violated, you'd have to prove that an individual is stalking you for personal reasons that are not in the public interest (for instance reporters and "paparazzi" photographers are legally allowed to "stalk" anyone who is legitimately newsworthy), or that they have malicious intent. **Public figures** such as politicians, actors, and celebrities have fewer legal privacy protections, so there is a greater burden of proof for legitimate violations of their privacy.

You can generally consider the following to be public information:

- Your full name
- Voter registration and political party affiliation

- Public records (court cases, real estate taxes and transactions, liens, judgements)
- Any details revealed in news stories
- Charitable and political donations
- Military service records
- Vehicle license plate numbers

All of the above aside, nothing else is considered public information unless you choose to make it public. For instance your phone number, home address, and email address will become public information if you publish them on your website or social media page. Also, you can choose to opt-out of public phone directory listings (insofar as those still exist) to prevent your otherwise unpublished phone number from automatically becoming public information.

To an extent – and subject to local and state laws – other people may legally be allowed to collect and publish your phone number, home address, email address, or other personal information that can be derived from public sources, unless their intent is to directly or indirectly cause you harm.[50] Unfortunately there is little you can do to prevent others from doing this anonymously; all you can control is what you choose to reveal publicly.

> ➢ NOTE: Do not assume that making your social media accounts "private" will prevent any information therein from being public. The moment you give your information to a third-party, you've permanently lost control over it.

Private Information

Private information is not necessarily a secret, but you would prefer it to be limited to your inner social circle of family and friends. Most information that falls into this category are things that you wouldn't think

[50] *https://kamanlaw.com/is-doxxing-illegal-in-the-u-s/*

anyone would benefit from knowing (or even be interested in), but you'd still prefer that they not be made public.

Depending on your personal information policy up until now, you may have made the following private information public, perhaps without realizing it:

- Age and date of birth
- Race / ethnicity / citizenship status
- Marital or relationship status
- Gender / sexual orientation
- Personal cell phone number
- Current and previous home addresses
- IP address
- MAC addresses of your connected devices
- Online aliases (usernames, player IDs, and handles)
- Your physical description (weight, height, hair color, facial hair, tattoos, scars, disabilities)
- Work address and desk phone number or extension (unless you've made a conscious decision to publish this information publicly for professional reasons)
- Current and past employment
- Names of the schools you currently or previously attended
- Group / fraternity / club affiliations

The above information should generally *not* be considered public by default, even if it is revealed in or by public records. It isn't that you want to prevent *anyone* from knowing these facts about you; it's that you don't want *any* fact about you to be collected and recorded in an automated fashion. If thieves, advertisers, and data brokers want to collect

information about you, then make them work as hard as possible to get it. Make yourself into an expensive person to collect data about.

The following should unequivocally be considered private information that you do not want to be published, and do not want anyone outside of your close friends and family to know:

- Driving record (beyond what is knowable from public records)
- Private health information (diseases, disabilities, injuries, conditions, prescriptions, treatments, inpatient status)
- Academic records
- Family tree / names of relatives
- Trust funds or large inheritances
- Relationship status and history
- Names of current and former pets
- Annual household income
- Credit score and history
- Your Internet and/or mobile service providers
- Purchase history
- Likes and dislikes
- Languages spoken
- Brand preferences

It's almost impossible to keep all of this information secret, but you're best served by limiting its publication (and therefore collection) as much as possible. On their own, none of these things is likely to lead to disaster if a motivated attacker is in possession of them. However, in collective this information can be used to reveal your secret information under certain conditions (I'll explain how later in this book), and it can certainly be used to influence you to make decisions that you would not otherwise make.

Secret Information

Secret information is nobody's business but yours (and perhaps your spouse's or parents'); it is information that you don't want anyone else to know unless it is critically important, and you never want it to be stored by third-parties (with the sole exception of zero-knowledge encrypted services like password managers). There are times when you will have to reveal secret information in order to complete a transaction of some kind, but often there are ways of revealing it that are not conducive to data collection.

Some examples:

- Social security number
- Bank account details
- Credit card numbers
- Confirmation of *any* customer account you have anywhere, even if it isn't an Internet-only service, for instance: utilities accounts, subscription services, online retailers, and warehouse club memberships
- Insurance policy details
- Usernames and passwords for sites, apps, and services
- PINs
- DNA / genetic data
- Addictions
- Cell phone / smartwatch IMEI and SIM numbers
- Any illegal or generally immoral activities
- Possessing firearms, expensive jewelry, recreational or commonly-abused drugs, large amounts of cash, or a safe or lockbox in your house or office
- Web search history

- Website visit history
- Anything you'd keep secret from your spouse, children, or employer
- Any information that would ruin your life, career, or relationship if it were publicly revealed

This doesn't mean that you need to live like a spy, but it is useful to think about how real spies operate.[51] In reality, espionage is nothing like James Bond, Jason Bourne, or Maxwell Smart.[52] Real "secret agents" don't go on epic adventures requiring science-fiction gadgets, guns, and martial arts; they mostly deal in bribery and blackmail.[53] In reality intelligence agents are not spies; rather, they *create* spies. Agents are mostly concerned with obtaining and selectively revealing secret information; they seek out ordinary people who have access to that information, and they convince them to become spies by exploiting their weaknesses and vices.[54]

Rather than attempting to work with a high-ranking government or military official, an intelligence agent is more likely to approach the low-profile people associated with them, then bribe or blackmail them into revealing secret information. This is why you can be denied a US Department of Defense security clearance if you have any vices (legal or illegal) or even a bad credit score; a high level of consumer debt is something that could be used as leverage against you by a foreign agent, as could a casual drug habit, alcohol addiction, marital infidelity, or gambling problem.[55]

The scope of secret information is much larger than most people imagine. If someone who seems like (but may not actually be) a police officer or Federal agent knocks on your neighbor's door, and your neighbor agrees to answer some questions about you, what will he or she say? How about your current and ex-spouses and partners? Current and former employers

---

[51] *https://www.cia.gov/stories/story/top-10-cia-myths/*
[52] *https://www.theatlantic.com/international/archive/2022/01/how-fake-spies-ruin-real-intelligence/621187/*
[53] *https://www.spymuseum.org/education-programs/spy-resources/espionage-facts/*
[54] *https://theconversation.com/how-ordinary-people-are-convinced-to-become-spies-166688*
[55] *https://veteran.com/rejection-security-clearance/*

and co-workers? Former classmates and teachers? Your children and their friends? Many of these people may be very close to you socially for a relatively short amount of time, and you have no control over what they may tell other people about you at any point in the future. You can't reasonably keep every piece of information about you a secret, but you can limit how much of it you share with people whom you know are not likely to be in your life for the long haul. Without resorting to dishonesty, you can be emotionally close to someone without revealing any secret information to them.

Very few readers of this book will ever need to get a Secret DoD clearance, or be recruited as a spy for a foreign government, but everyone should consider how their secret information could be used against them if it fell into the wrong hands:

- Debt collectors
- Lawyers and court process servers
- Jealous new partners of former lovers
- Jealous former partners of new lovers
- Jealous current partners of current lovers
- Stalkers
- Disgruntled former employees, co-workers, classmates, or roommates
- Professional thieves / career criminals
- People who feel they've been wronged by you or one of your family members
- A "social justice warrior" on a social media platform who believes that you (or someone who looks like you or has a similar name) are sexist, racist, or insufficiently accepting or supportive of gay or transgender people
- Criminals who are associated with your friends, co-workers, classmates, or family members

The last point is not to be taken lightly. It isn't about who you trust with secret information, it's about who they might tell after you tell them; this is, after all, *your* secret information, not theirs. If you mention to a co-worker that you keep $20,000 in cash in a safe in your house, and the co-worker casually mentions this at a party, a professional thief could overhear and decide to target you.

If your partner, friends, extended family, or children are aware of this information, instruct them to keep it secret; otherwise they may brag to their peers about your stealable assets, and that could attract the attention of criminals. Rarely do burglars randomly break into an unfamiliar house and then variously look for things to steal; most often they know (or know of) their victims, and have already done some reconnaissance and are expecting to steal specific things that are either untraceable or easily fenced, such as cash, drugs (legal or illegal), firearms, and jewelry.[56]

One of the oldest tricks in the burglary book is to masquerade as a door-to-door salesman or religious evangelist. What better way to "case the joint" than by being invited inside by one of the residents?

Assessing the Value of Your Information

Every piece of information about you has its own relative value or importance. In general, secret information will be more valuable than private information, and private will be more important than public – but not always – and even within each category there is a hierarchy of values.

For instance when you were 19 years old you may have been arrested and tried for a crime that is objectively disproportionate to its classification, such as operating a car while knowing that you do not have a valid driver's license, or being in possession of a small amount of marijuana. Depending on the jurisdiction, these could be misdemeanors or felonies, and many of the details of those court cases are freely available in municipal public records, where they can haunt you forever. There are many ways this data can harm you, even though it says little about your character and morals as a 45-year-old. For that reason, you could consider this data to be very high-value, even though it's in the lowest classification (public).

---

[56] *https://www.fbi.gov/news/press-releases/fbi-releases-2020-incident-based-data*

At the other end of the spectrum, you may have secrets that would be embarrassing if revealed publicly, but wouldn't ruin your life or harm your career, such as:

- Infertility, sterility, impotence, or frigidity
- The paternity of your children (if you adopted or used a sperm donor)
- Elective cosmetic surgery (liposuction, nose-job, breast enhancement or reduction)
- Falling victim to a scam
- Being closely related to a notorious criminal
- Working for a notorious company such as Phillip Morris, Enron, Arthur Andersen, The SCO Group, or Meta
- A past infection of genital warts or herpes
- Having a small penis
- Being a Seattle Seahawks fan

These may be secrets, and you may spend some effort protecting them from being published publicly, but they aren't truly *important* bits of information. If you could suddenly become omniscient, you'd be shocked at how many people you know who have secrets like these. While it would be embarrassing if this data were revealed publicly, it wouldn't be enough pain to enable blackmail, nor would it be likely to help an attacker gain access to your Google, Microsoft, or Apple accounts. You can't say the same for information that you may consider *public*, such as your name, address, phone number, and date of birth. However – as I show in Chapters 4 and 5 – even your most harmless-seeming secrets are valuable to scammers and corporate marketers because they reveal your interests and insecurities.

Transience, Expiry, and History

Traditional information security procedures require setting a time limit, after which a document must be re-classified. At that time, typically

something that has a very high classification will be demoted to a lower tier, or be destroyed; documents that begin in lower classifications may eventually be demoted to "public" because the data they contain is no longer useful to potential adversaries or bad-actors. For personal data this level of process is usually overkill, but there are some exceptions:

- Insider knowledge of information that will likely affect a publicly-traded company's stock value
- Availability of a scarce resource
- A medical diagnosis
- Anything that can be considered a "family secret"
- Searching for a new job
- "Spoilers" for shows and recent sports games
- Embargoed information (corporate information that has a planned future public release)

After a certain amount of time, most of these secrets can be safely revealed to your friends and family, or to the public, if they are no longer potentially damaging. To optimally protect your privacy, though, you must learn to expand the scope of transient personal data to include private and public information that is only important for a short amount of time, for instance:

- Your current location
- Timeframes when your house will be unoccupied
- If your car door is currently unlocked
- What you plan to eat for lunch today
- The brand and color of the shoes you're wearing
- The length, color, and style of your hair

Data can also change slowly because it lags behind current unrecorded information, such as:

- The age and condition of your car

- The value of your house
- Your weight, height, and age
- Your salary

If the gap between current personal information and current recorded data is great enough, it can cause trouble, such as when your appearance no longer matches your passport photo, or your signature on your driver's license has changed due to disability. Personal, governmental, and commercial correspondence may be delivered to old mailing addresses; password reset instructions may be sent to defunct email accounts or phone numbers; or you may lose out on a tax break, product safety recall notice, or class-action lawsuit payment.

Transient data does have some value when it is fresh, but there is often much more value in its history. Corporate marketers, scammers, and thieves can use your personal data history to establish patterns, and to predict future desires and behaviors. If possible, don't let them have it.

Anonymity is not Privacy

Privacy is the selective release of personal information. **Anonymity** is the quality of being nameless or unidentifiable. Obviously there is some overlap between the two, but they are not the same, and it's useful for you to start thinking of these as separate concepts. Anonymity requires privacy, but privacy does not require anonymity.

Never assume you are anonymous, and never rely on anonymity as a method of protecting your privacy. It only takes one clue to begin connecting your name to your online activity. Every criminal investigation begins with a named victim, an anonymous perpetrator, and a collection of clues that connect them, and most of the time the investigation ends with the arrest of a suspect who is linked to the crime by compelling and convincing evidence. Even "cold cases" and "unsolved mysteries" always have one or more likely suspects who cannot be formally charged solely due to a lack of good evidence.

Even if you can manage to remain totally anonymous on the Web, advertisers and search engines are still building profiles on you based on your search terms, clickstreams, time on site / page, and information

shared from "partner" cookies and trackers. While these companies may not know exactly who you are, they may know much about the anonymous person who uses your phone or Web browser, and – as I explain in detail throughout the remainder of this book – they will use that information to attempt to change your behaviors by showing you highly-targeted ads, altering your social media feeds, and sending you various kinds of spam.

Case Study: Superman

In the *Superman* comic book / TV / movie canon, Superman is a humanoid refugee from the planet Krypton who uses his super-human abilities to combat evil and save humanity from various catastrophes. As a baby he was adopted by a childless rural couple, and was raised as a normal human boy named Clark Kent. Later in life Clark became a journalist, and decided to secretly develop a separate persona named "Superman" so that he could use his superpowers to help people without ruining his journalistic integrity or subjecting his adoptive parents to harassment from the paparazzi.

Superman is not anonymous; everyone in Metropolis can identify Superman by his iconic costume and his superpowers. Clark Kent is also not anonymous, which is evidenced by the fact that we know his name (Clark Kent) and where he works (a newspaper called *The Daily Planet).* However, Superman / Clark Kent is *very* good at protecting his privacy. He even has a different set of controls for both his superhero and alter ego identities, which is an underrated superpower considering both Superman (as a "public figure") and Clark Kent (as a member of the news media) are legally less entitled to privacy than ordinary citizens:

- No one knows where Superman lives, but you can find Clark Kent's home address in the local phone directory.
- Superman has no public records because he earns no income, owns no real property, isn't registered to vote, and doesn't have a passport or driver's license; Clark Kent has a state-issued ID, a corporate-issued press pass, a car, years of tax returns and school records, and is named in the masthead and/or article bylines in every issue of *The Daily Planet.*
- Superman is not very good at keeping his disability (vulnerability to kryptonite) a secret, whereas Clark Kent successfully feigns a disability (poor eyesight) by wearing superfluous eyeglasses.

- Superman's superpowers are obvious and on public display, yet as Clark Kent he must consciously reduce them so that no one will notice that he's super-human.

Who, then, *is* anonymous in this fictional reality? How about the guy who says: "It's a bird! It's a plane! It's Superman!" No one knows who that guy is, what he does, where he lives, or why he can't tell the difference between birds, airplanes, and a flying alien in a blue and red spandex costume.

What's Most Dangerous?

As I'll explain in the next chapter, the foundation for the most damaging direct threats that can result from poor information security practices is **identity theft** (when someone else has enough information to credibly impersonate you in an official capacity). The minimum information required for many forms of identity theft is:

- Full name
- Date of birth
- Current home address

And the more of the following information a thief has, the more harm he or she can do with fewer resources and skills:

- Social security number
- Medicare account number
- Numbers for your various financial accounts, cards, and forms of ID
- Phone number
- Name of employer
- Previous home addresses
- Email address
- Usernames and passwords for online accounts

The documentation required to successfully perpetrate identity theft falls into two categories. Official:

- Birth certificate
- Death certificate
- Driver's license
- Vehicle registration, title, or license plate
- Passport
- Military ID
- Student ID
- Social Security card
- Voter registration card

And unofficial (not issued by a government agency):

- Consumer credit report
- Signed lease agreement
- Utility bill (including cellular phone and Internet service)
- Bank or brokerage statement
- US Postal Service "change of address" letter
- Offer of employment letter
- Proof of insurance (health, dental, vehicle)

The information that appears on any two of the above-listed documents (whether they are genuine or fake) is usually enough for most identity thieves to work with.

Who's Collecting It?

In order to assess your risks, you must understand the people and entities that are willing and capable of exploiting your personal or private information, how they collect it, and how they benefit from it.

At one end of the spectrum are **large corporations that exploit user data for marketing or advertising purposes.** They seek to help their clients manipulate you into making a decision that you wouldn't ordinarily make, such as what to buy or who to vote for in an election. Such companies are usually limited in the data they are allowed to access and collect. Facebook, for instance, isn't going to pull your credit report or parse through court cases; such information is expensive to access, and is unlikely to yield enough extra conversions for the ads it typically sells.

The most dangerous ads on social media and search engines are **influence campaigns** (large-scale marketing efforts that use a variety of tactics to alter public opinion on a certain topic), which benefit from accessing simple personal data, though they can only work on people who are able to be influenced. The long history of the marketing industry has proven that most people can be convinced to change their minds about most things if they are repeatedly exposed to effective propaganda. However, simply being aware of the existence of influence campaigns provides a certain level of resistance to them, so let me be clear: <u>everything you see in any advertisement anywhere is an attempt to influence you.</u> This includes **product placements** (conspicuous inclusion of a certain brand or product in a social media post, TV show, movie, or other visual medium).

At the opposite extreme are **motivated attackers** such as stalkers, law enforcement, and private detectives. They have a single target in mind: you. That means that they are willing and usually able to access private information from both commercial and public sources. Law enforcement can gain access to nearly any data it needs from any source, so long as there is probable cause and/or a warrant. Stalkers are already breaking the law, so they may be willing to obtain private information through illegal means such as a Dark Web database of stolen data, or by paying for detailed court or vehicle records (while it is not usually illegal to access that information for most purposes, it is illegal to access it for nefarious purposes). Private investigators may have legal access to some private data that would ordinarily be out of reach for a stalker, such as any information given to them by their client. A private investigator is also legally allowed to follow

and secretly record or photograph someone's public activity. The worst-case scenario among motivated attackers is a law enforcement officer who is also a stalker, and therefore has access to legally-protected private information on their victims; this is not as rare an occurrence as it should be, unfortunately.

Between these two extremes are a variety of businesses that seek to use personal information for financial gain. Some will sell your data to individuals or other companies; some will sell access to data-sorted cohorts of people to their advertising clients; some will mostly use your data to **drive engagement** (encouraging, coercing, compelling, or manipulating users to spend as much time as possible profitably interacting with an app or service).

Every time you type anything into a Web form, app, or search field; fill out a paper form; allow something to be photocopied (such as your driver's license); or purchase something with a credit or debit card; assume it is being collected and associated with you, and will be used against you in the future.

Governments

For a variety of regulatory and bureaucratic reasons (most notably taxes) every government agency at every level (local, state, national) collects personal information about the people who live there. Unfortunately they aren't always able to keep that data secure, but aside from voting for laws, policies, and candidates that promote better information security, there's nothing you can do about that.

All of the information that Western (or more broadly, democratic) governments collect about their citizens is classified as an official record controlled by strict regulations that specify what is recorded, where it is stored, how long it is retained, and who can access it. Some of it is a **public record**, which is generally available to anyone upon request (though in some instances it may only be available to view in person at a government office, not online); more sensitive information is only available to public servants, elected officials, or appointees of specific agencies on a "need to know" basis and cannot be published elsewhere or shared or used for any reason other than the one given, or it is only obtainable by legal request (such as a warrant or order).

A surprising amount of personal and private information can be included in public records:

- Vehicle registration (including your VIN; license plate; and year, make, and model of your car)
- Driver's license (including your physical description, home address, and date of birth)
- Real property sales and tax assessments (including the address of the property, the name of the buyer and seller, and the sale price history)
- Court cases (though portions of court documents may be redacted or sealed by a judge, and past cases can be expunged upon reasonable request)
- Arrest records
- Business filings
- Voter registration (including political party affiliation and voting district)

Autocratic regimes – most notably those in control of rogue nations such as China and Russia – collect personal data on their own people to censor public speech, quash potential uprisings, and root out foreign clandestine assets; and they commit data breaches in the US and other countries to steal trade secrets from technology companies and to identify foreign agents and recruit domestic spies. According to the FBI and the US Department of Justice, the largest data breach in history (Equifax in 2017) was committed by members of the Chinese military, likely for intelligence and counter-intelligence purposes; the data has not, as of the publication of this book, been made available on the Dark Web, nor is there any indication that it was used to commit financial crimes or identity theft.[57]

In the US, the biggest data collectors are three-letter agencies, including the TSA and IRS. Their intentions are obvious and usually transparent – collecting taxes, fighting terrorism and organized crime, and conducting counter-intelligence on foreign agents. However, the FBI and NSA have

[57] *https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020*

been caught misusing personal data for blatantly off-mission and illegal reasons: the FBI under J. Edgar Hoover surveilled, harassed, burglarized, and even blackmailed people who were not suspected of committing crimes, including Martin Luther King, Jr.[58], Muhammed Ali[59], and John Lennon[60]; and more recently the NSA (with extra help from tech companies and cellular service providers) was caught spying on American citizens who weren't terrorism suspects or foreign agents.

Case Study: Warrentless Wiretapping Yields Nude Photos

In 2013, a US citizen and employee (or contractor) of the National Security Agency named Edward Snowden publicly revealed the existence of a massive secret domestic surveillance system officially known as SIGAD US-984XN, or informally as PRISM or "warrantless wiretapping."[61] The program enabled the NSA to monitor and record all online, SMS text, and voice call content on all Americans.

Technically the law only allows recording communications that cross the US border – if a US resident calls, texts, or emails someone outside the US – but networks often invisibly cross national boundaries without warning, and datacenters for US-based services may be located in other countries without users' knowledge. So if, for instance, Google were to move some Gmail user data from one datacenter to another, if any part of that digital journey crosses the US border, then the NSA will copy, analyze, and archive it. That means everything you've stored online (unless it's end-to-end encrypted with a zero-knowledge service provider as explained in Chapter 2) or communicated to anyone else in any electronic format since approximately 2007 (and any phone conversations you had long before that) may have been (or will someday be) viewed, read, or heard by an NSA agent.[62]

---

[58] *https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/*
[59] *https://en.wikipedia.org/wiki/COINTELPRO*
[60] *https://www.cia.gov/readingroom/document/cia-rdp91-00587r000100370003-0*
[61] *https://en.wikipedia.org/wiki/PRISM*
[62] *https://arstechnica.com/tech-policy/2013/09/loveint-on-his-first-day-of-work-nsa-employee-spied-on-ex-girlfriend/*

The NSA does not act alone; it can compel technology and telecommunications companies to provide access to any data they store or transfer, and by law no one at those companies is permitted to speak publicly about it. According to investigative reporting by *The Guardian,* the following companies are known to have supplied user data (or unrestricted access to it) to the NSA:[63]

- Verizon
- Microsoft (including Skype and Hotmail)
- Apple
- Google (including YouTube)
- Facebook
- Yahoo (including AOL)
- Paltalk
- Dropbox

There is an ongoing debate as to the constitutionality of this program, and whether the NSA has been properly following the law that regulates and governs it. Certainly it is a massive violation of every American's privacy, but according to Snowden, it was even more invasive for people who stored or transferred (unencrypted) nude photos of themselves; allegedly some rogue NSA analysts considered it a "fringe benefit" to actively search for and share nude pictures of attractive women while they were supposed to be looking for evidence of terrorism:[64]

[63] *https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*
[64] *https://www.pcmag.com/news/watch-snowden-explains-how-the-nsa-can-see-your-naked-pics*

You've got young enlisted [military] guys, 18 to 22 years old. They've suddenly been thrust into a position of extraordinary responsibility where they now have access to all of your private records. In the course of their daily work they stumble across something that is completely unrelated to their work in any sort of necessary sense. For example, an intimate nude photo of someone in a sexually compromising position. But they're extremely attractive.

So what do they do? They turn around in their chair and show their co-worker. The co-worker says: 'Hey that's great. Send that to Bill down the way.' And then Bill sends it to George and George sends it to Tom. And sooner or later this person's whole life has been seen by all of these other people. It's never reported. Nobody ever knows about it because the auditing of these systems is incredibly weak. The fact that your private images, records of your private lives, records of your intimate moments have been taken from your private communications stream from the intended recipient and given to the government without any specific authorization without any specific need is itself a violation of your rights. Why is that in a government database?

-Edward Snowden[65]

As of the publication of this book, the PRISM program is believed to still be in operation; it's reasonable to assume that it now includes data from

[65] *https://arstechnica.com/tech-policy/2014/07/snowden-nsa-employees-routinely-pass-around-intercepted-nude-photos/*

many more tech and telecommunications companies than the ones I've listed above.

Banks, Credit Agencies, and Data Brokers

When you open a new account at a bank, brokerage, or lender, the KYC information you provide will be checked against one or more credit files held by **data brokers** (companies whose primary business is collecting and selling personal data) such as: Experian, Transunion, Equifax, Acxiom, Epsilon Data Management, Oracle, Verisk, Lexis-Nexis, CoreLogic, and ChexSystems, among many others that serve niche markets. If there are any discrepancies between the information you provide and what's recorded in your credit files, you will be denied credit or be asked to provide additional personal information (most commonly other forms of identification). Banks in specific are required to notify you of credit decisions by US mail only; if you get an email, text, or phone call from someone claiming to be from a bank, assume that it is a scam.

The information in your credit files originates not only from creditors (such as banks and mortgage lenders), but also any other entities that make judgements about you based on various aspects of your documented history (such as insurance companies, landlords, schools, and employers), so you can expect that any extra information you provide in any kind of application will end up in your credit report and any number of other databases. Your employer can report the date range of your employment, salary or pay rate, job title, and the division or department you work in.[66] Your University can report your enrollment and degree information. If you rent, your landlord can report if you're late on a rent payment or if you have an unauthorized pet.[67]

Your personal information is extremely valuable to data brokers and their clients; the industry pulls in about $200 billion annually.[68] Sometimes the data they collect is free, and sometimes they pay other companies for their customer or user data, then they create an aggregate from all of those sources, and sell it to anyone who's willing to pay for it.

---

[66] *https://theworknumber.com/resource/-/resource/the-work-number-portfolio-review-product-sheet*
[67] *https://www.thelpa.com/lpa/ntrb_description.html*
[68] *https://privacy.com/blog/what-are-data-brokers*

The amount of data collected and analyzed by data brokers is so substantial that even Federal agencies like the FBI and DHS sometimes find it cheaper and easier to purchase personal data from a data broker rather than request it through a warrant or collect it on their own.[69] Thieves and blackmailers don't even need to execute a data breach or buy a stolen data cache from the Dark Web; they can legally purchase most of what they need from a data broker (though President Biden signed an executive order in 2023 that prohibited data brokers from selling data to anyone who is in or has close ties to "countries of concern").[70]

Social Media

I've made it pretty clear throughout this book that social media companies collect, use, and sell as much personal data as possible, so instead of repeating what's already been written, I offer you this excerpt from a text conversation between Mark Zuckerberg and a friend during the early days of Facebook:[71]

> *zuckerberg: Yeah so if you ever need info about anyone at Harvard*
>
> *zuckerberg: Just ask.*
>
> *zuckerberg: I have over 4,000 emails, pictures, addresses, SNS*
>
> *friend: What? How'd you manage that one?*
>
> *zuckerberg: People just submitted it.*
>
> *zuckerberg: I don't know why.*
>
> *zuckerberg: They "trust me"*

---

[69] *https://www.businessinsider.com/lawmakers-investigate-company-selling-phone-location-data-to-the-fbi-2020-6*

[70] *https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/*

[71] *https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/*

zuckerberg: Dumb fucks.[72]

Hospitals and Health Care Providers

Federal regulations prohibit health care providers from sharing patient information with third-parties, with two exceptions: when the patient specifically allows it (for instance when you want your medical records sent from one doctor's office to another's), and when it is **de-identified,** which means that the following **protected health information** (PHI) is not included in a patient's medical record:[73]

- Name
- Date of birth
- Home address
- Telephone or fax number
- Social security number
- Vehicle identification of any kind (VIN, license plate, registration, license)
- Dates, except for the year
- Geographic location beyond the first three digits of the ZIP code
- Device identifiers and serial numbers
- Email address
- URLs (when they can identify a patient)
- IP addresses
- Medical record or patient ID numbers
- Biometric identifiers (fingerprints, retina scans, etc.)

---

[72] *https://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5*

[73] *https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html*

- Insurance, Medicaid, or Medicare ID numbers
- Account numbers of any kind
- Photographs of the patient
- Certificate or license numbers

That seems fairly comprehensive in terms of keeping a patient's identity out of his or her shareable / sellable medical records, but it can still lead to serious privacy violations and even identity theft because de-identified data can easily be re-identified by combining it with data from other sources.[7475] Furthermore, third-party services that "partner" with healthcare providers for things like Web portals or mobile apps may not be subject to Federal HIPAA regulations.[76]

Somehow, while there are restrictions on sharing or selling "de-identified" health data to third-parties, as of the publication of this book there is no Federal regulation prohibiting healthcare providers from using patient data for their own marketing purposes.[7778] So if you visit a hospital to get an MRI or a biopsy, you can expect its parent company to use every piece of personal information you gave it to spam you indefinitely (unless the US Federal Trade Commission introduces a new rule to address it before this book goes to print).

Healthcare providers often ask patients to provide personal information that is not relevant to the service they are requesting. It's reasonable to assume that any information you provide will be used by the healthcare provider and its "partners" for marketing purposes; therefore I suggest that you provide only the bare minimum necessary for medical treatment (your name, date of birth, insurance / Medicaid / Medicare policy information, and perhaps your mailing address). Unless you are a military

---

[74] https://www.accountablehq.com/post/medical-marketing-hipaa
[75] https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research
[76] https://www.washingtonpost.com/technology/2019/10/22/help-desk-can-your-medical-records-become-marketing-we-investigate-readers-suspicious-patient-portal/
[77] https://www.beckershospitalreview.com/digital-marketing/the-uncharted-waters-of-using-healthcare-data-for-marketing-practices.html
[78] https://www.linkedin.com/pulse/leveraging-patient-data-targeted-marketing-campaigns-abou-nabbout-psf4f?trk=public_post

veteran seeking treatment at a VA facility, you do not need to provide your social security number to any healthcare provider; if they insist, or if they use apps or Web forms that require your SSN, use dummy information (as explained in Chapter 2).[79] It may benefit you to provide a phone number or email address if you want to be notified of the availability of test results or scheduling changes, but you can just as easily call the office yourself to check on results or confirm an appointment. You do not need to disclose your race, ethnicity, sexual orientation (though prior to 2023, gay men were prohibited from donating blood), occupation (unless your visit pertains to a job-related injury or workman's compensation claim), or annual income. Marital or relationship status is somewhat of a grey area; some states require this information from mothers who are giving birth, to determine legal paternity; it may also be used to determine next-of-kin or a legal decision-maker in situations where a patient is unconscious.

In an emergency there is no time to read through multiple pages of legalese before receiving life-saving treatment. It's likely that many (especially for-profit) hospitals slip in a few consent forms that enable them to collect, use, and sell your (or your loved-one's) personal information, but this is not the time to argue in favor of your data rights, and if it should come to litigation in the future, such underhanded tactics (being forced on you "under duress") are unlikely to be viewed favorably by civil court judges in most jurisdictions. When every second matters, just sign the forms.

The other side of the healthcare data coin is focused on doctors, not patients. Pharmaceutical companies collect as much medical data as possible, then use that to target doctors and other healthcare providers with marketing that influences them to prescribe certain medications.[80]

Case Study: Medical Transcription Blackmail

Back in 2003, the University of California at San Francisco (UCSF) Medical Center received a blackmail threat via email: "Your patient records are out in the open… so you better track that person and make him pay my dues."[81] The blackmailer, a woman in Pakistan named Lubna Baloch,

---

79 https://www.consumerreports.org/electronics/personal-information/if-doctor-asks-for-social-security-number-a1084748956/
80 https://www.ncbi.nlm.nih.gov/books/NBK236546/
81 https://www.sfgate.com/health/article/a-tough-lesson-on-medical-privacy-pakistani-2552427.php

followed up with proof: an email containing UCSF patient records. At first this looked like an ordinary blackmail attempt, but further investigation proved that it was a much bigger problem.

Lubna Baloch wasn't in the business of blackmailing hospitals; she was a transcriptionist who typed out notes that doctors had recorded on tape – a practice that is still largely used today in the medical industry, though dictation is now usually recorded digitally rather than on analogue tape recorders. When medical facilities don't use speech-to-text software for transcription, they usually outsource the labor to a third-party agency that employs contractors. In this case, that third-party agency was Transcription Stat, based in Sausalito, CA, and it had given UCSF's transcription work to a sub-contractor in Florida named Sonya Newburn. Apparently unbeknownst to UCSF and Transcription Stat, Newburn outsourced her transcription work to a cheaper subcontractor in Texas named Tom Spires, who (allegedly unbeknownst to Newburn) outsourced the work to even cheaper subcontractors, one of whom was Pakistan-based Lubna Baloch.

When Spires refused to pay Baloch for her work and cut off all contact with her, Baloch emailed her blackmail threat to the hospital, apparently believing that Spires was either an employee or in direct contact with the hospital. UCSF officials, however, had no idea who Tom Spires was or why he was sending their medical records to an offshore subcontractor. Sonya Newburn was eventually able to unwind the mystery and offered to make a partial payment directly to Baloch, with the condition that she retract her threat. Baloch agreed, and sent another email to UCSF: "I verify that I do not have any intent to distribute/release any patient health information out and I have destroyed the said information. I am retracting any statements made by me earlier." Unfortunately there was no way to verify that she followed through on her promise.

Though medical transcription work is increasingly being done by speech-to-text software, healthcare providers still outsource some transcription work (and other things, such as apps that facilitate records-sharing and patient communication) to third-party providers who may, in turn, outsource some of their processes to other third-party contractors and companies. In other words: similar problems could happen again and, as illustrated in the next case study, they already have.

Case Study: Blackbaud Blackmail

Blackbaud is an American company that specializes in a variety of Web- and cloud-based services for more than 45,000 non-profit companies, healthcare organizations, educational and religious institutions, and other corporations in the US, EU, and Canada. Its flagship products focus on managing databases of donors, clients, and patients for fundraising purposes, and in many of those market segments it has very little direct competition. If you've donated money to any charitable organization in the past 15 years, there's a good chance that Blackbaud was involved somewhere behind the scenes. Blackbaud's customer databases can contain a wide variety of critical personal information, including medical records, social security numbers, and bank account details.

The risks of storing this kind of information are clear and obvious; unfortunately Blackbaud's executives didn't take them seriously enough. A substantial amount of customer data, including social security numbers, bank account details, and external files containing other personal information, was often stored and transmitted without encryption. Database backup files containing all of that data were also stored unencrypted. Even worse: some of that personal information was kept on Blackbaud's servers when it should have been deleted; Blackbaud had no legitimate business reason to retain it at all, let alone for several years.

In May of 2020, hackers used a Blackbaud customer's login information to break into the databases of tens of thousands of other customers, which gave them access to the personal information of millions of people who almost certainly had no idea that Blackbaud even existed, let alone was entrusted with securing their personal data.[82] When Blackbaud employees finally discovered and cut off the data breach, the attackers demanded a ransom of 24 Bitcoin (approximately $250,000 at the time). Blackbaud paid the ransom, but was unable to verify that the stolen data had been deleted as promised.

It was July before Blackbaud partially disclosed the breach and ransom payment, but at first it downplayed the severity of the incident in a statement to its customers: "The cybercriminal did not access credit card information, bank account information, or social security numbers. . . No

[82] *https://www.ftc.gov/business-guidance/blog/2024/01/ftc-says-blackbauds-lax-security-allowed-hacker-steal-sensitive-data-thats-just-beginning-story*

action is required on your end because no personal information about your constituents was accessed."

Unfortunately that statement was false, and it misled Blackbaud's clients about their obligation to report the data breach to their customers and donors, many of whom claimed that they'd been the target of identity theft and financial fraud likely stemming from the Blackbaud breach. In September 2020 the company finally revealed (via its SEC form 8-K filing) the full extent of the personal data that had been stolen. The delays in reporting the incident and its severity were in violation of several US and EU regulations, and Blackbaud was fined millions of dollars by the EU and the US SEC, and settled a class-action lawsuit from 49 US states and the District of Columbia for $49.5 million.

In February 2024, the US FTC filed a detailed complaint against Blackbaud, demanding that the company be required to delete any consumer data it no longer needs, implement a comprehensive information security program, and mandating a data retention schedule that explains how and why Blackbaud maintains its databases and when data will be deleted. As part of the proposed order, Blackbaud must also directly and promptly notify the FTC of any future data breaches. As of the publication of this book, the FTC order has not yet been finalized and executed.

Big Tech

In Chapter 2 I listed all of the personal information that Alphabet and the providers of other "free" services collect. Everything you search for, click on, or otherwise interact with on any platform provided by a company that shows digital ads or sponsored content is being collected, analyzed, and used for the purpose of targeting you (as specifically as possible) with ads that you're likely to be receptive to. Those ads are not necessarily shown in the apps or services where they're collected; for instance Microsoft may collect data from Windows users that is used to show them ads on Bing or Outlook.com. There is a staggering amount of money in this practice. As of 2023, about 76% ($65.5 billion) of Alphabet's revenue and 96% of Meta's revenue comes from user-targeted advertising; keep that in mind the next time you search YouTube for a video, or "Google" something

while signed into your Google and Facebook accounts in other browser tabs.[8384]

Search engines are not the only products owned by Alphabet and Microsoft. In addition to many other software, hardware, and service products, both companies own the world's most-used operating system software in Android and Windows, respectively. It's unknown exactly what data Microsoft and its third-party "partners" are collecting from computers running Windows version 11, and what that data is being used for beyond the development and deployment of security patches and product updates, but I do know that quite a bit of it is being sent from users' PCs to a variety of destinations.[85] On Android devices, invasive apps such as Facebook, Instagram, and the full suite of Google apps are typically installed on (and often can't be completely removed from) mobile devices, though this is sometimes done by the device manufacturer or wireless carrier as a result of pay-to-preinstall agreements.

Similarly, Alphabet and Apple frequently receive a variety of information from connected mobile devices that use their operating systems, as do many of the companies that make the apps installed on them.[86] While this data in isolation may not always be personally-identifiable, it can easily be associated with other personal data that those companies collect. Alphabet in particular keeps mobile telemetry data in a database it calls **Sensorvault**; this data can easily be requested by law enforcement to identify the owners of mobile devices in a given geographic area. As I show in Chapter 4, this sometimes results in innocent people being investigated and even arrested for crimes they didn't commit, simply because Sensorvault data showed that their smartphone was detected in the vicinity of a crime. Apple claims that it does not routinely retain device telemetry on that scale, but it does cooperate with valid legal requests from law enforcement.

---

[83] *https://www.gurufocus.com/news/2325851/meta-platforms-had-a-banner-year-in-2023*

[84] *https://www.sec.gov//Archives/edgar/data/1652044/000165204424000014/googexhibit991q42023.htm*

[85] *https://www.tomshardware.com/news/windows-11-sends-user-data-to-third-party-services*

[86] https://arstechnica.com/gadgets/2021/03/android-sends-20x-more-data-to-google-than-ios-sends-to-apple-study-says/

Alphabet, Microsoft, and Apple also have large-language model (LLM) artificial intelligence (AI) products that are trained chiefly by pulling text from publicly-accessible websites and books.[87] Anything you've published on the Web or in print may have been used (without your knowledge or permission) to train an AI model. As of the publication of this book, it isn't yet known what the impact of this practice may be on people's privacy and copyrights, but copyright infringement lawsuits are pending (and many more may be filed in the future) against the tech companies that use these methods to develop their AI products.

Before you started reading this book, you were probably at least somewhat aware of the personal information collection practices of big tech companies like Alphabet and Meta, but it's not just the usual suspects you should be cautious of. Nearly every modern company that relies on complex technology solutions to squeeze more money out of its customers is heavily invested in collecting and using personal data for advertising or marketing purposes. This book is rife with examples, but here are a few others that you may not know about:

- **Uber** uses your personal information, including your current location and your ride destination, to show you targeted ads in its app while you're a passenger.[88]

- **Marriott** sells / shares customer and rewards program data with its advertising "partners" to show travellers personalized ads "throughout their path of purchase, pre-arrival, and during their stay" via a wide variety of mediums, including the televisions in its hotel rooms, and its mobile apps and other services.[89]

- **United Airlines** is, as of the publication of this book, "considering" using customer data to show ads targeted to each ticketholder on its in-seat screens.[90]

---

[87] *https://copyrightalliance.org/ai-copyright-courts/*
[88] *https://www.theatlantic.com/technology/archive/2024/02/online-ads-more-annoying/677576/*
[89] *https://news.marriott.com/news/2022/05/16/marriott-international-introduces-travel-media-network-powered-by-yahoo*
[90] *https://www.wsj.com/business/airlines/united-airlines-weighs-using-passenger-data-to-sell-targeted-ads-21ddb447*

Targeted ads are extremely effective compared to conventional marketing methods. In Chapters 4 and 5, I explain the many ways that data-driven advertising can harm the people it targets.

Car Manufacturers

As vehicles become more reliant on software for features and services, their manufacturers – to varying degrees – help themselves to as much personal data as they can possibly collect from their drivers. Even worse, some manufacturers have partially or completely given up on trying to develop their own in-car operating system software, and instead assume that every driver will connect his or her smartphone and use either Android Auto or Apple CarPlay, enabling Google and Apple to potentially record any information about your car, location, and travel habits that they grant themselves permission to access.

Even without connecting a smartphone to your car, the manufacturer can and will collect a surprising amount of data from you. According to a comprehensive analysis by the non-profit Mozilla Foundation, "cars are the worst product category we have ever reviewed for privacy."[91] Though all car manufacturers collect, use, and sell or share a large amount of owner / user data, the most extreme example I could find is Nissan which, in addition to vehicle usage data, grants itself permission to collect, use (for marketing and "operational" purposes), and share or sell (with / to an unlimited number of third-party "partners" in an "anonymized" fashion, which is neither explicitly defined nor accessible to audit by owners / drivers) the following personal information from people in the North American market who buy and/or use its cars:[92]

- Race
- National origin
- Religious or philosophical beliefs
- Sexual orientation
- Sexual activity

[91] *https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/*
[92] *https://www.ft.com/content/dd4d11e4-282a-46f9-9234-963374165fe5*

- Precise geolocation
- Health diagnosis data
- Genetic information

As for calculated data (this term is defined in detail in the "How Is It Collected?" section later in this chapter), Nissan reserves the right to "draw inferences about psychological trends, behaviors, attitudes and intelligence" of owners / drivers.

Insurance Companies

Along with moneylenders, insurers are the original personal information hoarders, going all the way back to the days of paper records, local gossip, public reputations, family connections, and handshake agreements. Insurance companies are fundamentally in the business of making financial guarantees based on risk, and are therefore eager to collect and analyze as much information about policyholders and their assets as possible. Despite their wealth of data, though, they still cannot predict the timing and severity of accidents and other random events that lead to claims; personal data is not a crystal ball. At best, probabilities can be calculated based on broad generalizations of cohorts, which is inherently discriminatory. For instance an insurance company or a data broker that sells analytics to insurers may determine that, all else being equal, someone with a 4-year college degree is less of a risk than someone who didn't attend college. Based solely on that statistic, the insurer may decide to charge higher rates for non-college graduates. There is an ongoing debate among regulators and the insurance industry as to what forms of discrimination are legally allowed in underwriting, and how much transparency there is or should be in the algorithms that assess risk and calculate rates.[93]

As detailed in the previous section, the data collected by your car's manufacturer is almost certainly being sold to data brokers, who in turn sell it to insurance companies, who then use it to adjust your auto insurance

[93] *https://www.investopedia.com/insurance-underwriting-guidelines-discrimination-5203311*

rates.[94] Unfortunately for you, the data doesn't necessarily specify who is driving the car at any given time, or if there is an emergency.

Many car insurance companies offer discounts to customers who agree to use a telemetry device or mobile app that constantly records driving activity. If you participate in one of these schemes, I hope that you're mindful to never let anyone else drive your car, you're lucky enough to never have your car stolen by joyriders, and you never have to rush to the hospital for an emergency.

Internet and Cellular Service Providers

Most service providers are fundamentally interested in determining, through analysis of personal data, whether a prospective customer is going to pay his or her bill in full and on time. For this purpose, a standard consumer credit report is usually sufficient. However, Internet and cellular service providers are increasingly becoming data brokers, collecting as much information about each subscriber as possible, including their Web history, mobile app usage, and realtime device location data, and selling it to third-parties such as other data brokers, online advertisers, bail bondsmen, bounty hunters, property managers, and car salesmen.[95]

Even if you use a privacy-focused Web browser, you can assume that every app you use and every website you visit is being recorded by your ISP, primarily for marketing purposes. Fortunately much of this data can be blocked or obscured by implementing all of my recommended privacy and security practices in Chapters 1 and 2. To a limited extent, ISPs also offer the opportunity to opt-out of some of their data collection and sharing practices; this is covered in detail in Chapter 6.

DNA Testing and Ancestry Tracing Services

DNA-based ancestry tracing services like AncestryDNA (Ancestry.com), GenoPalate, MyHeritage, and 23andMe can provide fascinating insights on your genetic roots, medical risks, and potential distant relatives. Unfortunately, some of them are collecting and selling not only your

---

94 https://www.digitaltrends.com/cars/car-insurance-companies-data-collection/

95 https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few

genetic data, but all personal information you provide via their websites, various data collected by using their mobile apps, and any other data the company has access to, including: newspaper articles, birth records, immigration lists, and social media services. DNA data aside, DNA testing and ancestry tracing companies are just normal technology corporations in that they collect as much personal information about you as possible, then use it against you (and/or sell it to another company) for marketing purposes.[96]

These companies usually promise not to share your genetic data, or to only share it in a "de-identified" fashion (and as with all "de-identified" data, it can be easily re-identified by combining it with other data), or to only share it if you choose to let them share it for "research" purposes. Unfortunately the term "research" in this context is much broader and more invasive than most people imagine. While your DNA information may be used by legitimate medical researchers, academics, and scientists for virtuous purposes, buried in the fine print you may discover that any information the company collects about you – not just your DNA data – can be sold, shared, or used for a variety of "research" purposes that have nothing to do with the advancement of medical science.

Law enforcement can (and often do) obtain DNA data and other personal information from these services with a warrant. More commonly, though, the police are customers of these services; they send in DNA samples from crime scenes or evidence kits, and the DNA service provides either a direct match or a list of close relatives.[97] Once the cops have that list, they can ask a judge to legally compel the service to provide more information, or use other methods to contact those people with the hope that they'll provide more details about the suspect. On the one hand, we all want criminals to be caught and arrested quickly; on the other hand this is a massive invasion of privacy, and exposes innocent people to investigation or interrogation because a potential relative's DNA was found at a crime scene. DNA is not a "smoking gun;" like any other physical evidence, alone it often suggests nothing because any number of people could have unintentionally left their subtle genetic mark on a crime scene before or after the crime was committed. As with all scenarios in which one could

---

[96] *https://www.consumerreports.org/health/dna-test-kits/privacy-and-direct-to-consumer-genetic-testing-dna-test-kits-a1187212155/*

[97] *https://www.aclu.org/news/privacy-technology/police-need-a-warrant-to-collect-dna-we-inevitably-leave-behind*

say "If you haven't done anything wrong, then you have nothing to hide," you must consider the potential for authorities to use these powers for selfish reasons, which – as I've already described in this chapter (and there's more on this subject in Chapter 4) – they occasionally do.

If you do choose to use one of these services, I recommend not opting-in to sharing your data for "research" (or any other) purposes. I also urge you to consider what would happen if, through DNA testing, you were to discover some unexpected piece of information that would cause harm. Since their inception, DNA testing services have fueled a constant supply of news stories about customers who discovered that one or more of their immediate family members were not biologically related to them, resulting in long-term trauma, anxiety, and family discord.

Case Study: 23andMe Blames Its Customers For Its Data Breach

In October 2023, DNA testing company 23andMe revealed that hackers had stolen ancestry data from about 14,000 of its user accounts. Furthermore, those compromised accounts had enabled the attackers to copy 6.9 million user profiles (almost half of its userbase), which provided the following personal information:[98]

- Full name and family surnames
- Profile photo
- Ethnicity estimates
- Some DNA information (mitochondrial DNA haplogroup and Y-chromosome DNA haplogroup)
- Grandparents' birthplaces
- Birth year
- Relationship status

[98] *https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/*

- Percentage of DNA shared with the relative whose account was compromised
- Ancestry reports
- Self-reported information such as location and freeform "about" notes

23andMe spokespeople insisted that this information "could not have been used to cause pecuniary harm" because it did not contain social security or driver's license numbers, or payment information. Regardless, more than 30 lawsuits were filed against it by users whose personal information had been stolen.

The stolen data ended up for sale on the Dark Web, at first in two cohorts that specifically identified Ashkenazi Jews and people of Chinese descent, then millions more records a few weeks later.

Unlike most data breaches, this was not an attack on the 23andMe infrastructure; it was a brute force attack (this concept is covered in detail later in this chapter in the "Methods of Intrusion" section). 23andMe only required a simple username and password for account security, and those 14,000 compromised accounts had reused passwords from other sites that had been exposed in other data breaches. (This is why I urged you to use a good password management tool and to review and update every one of your online accounts with unique strong passwords in Chapter 1. If you didn't do that earlier, then put a bookmark here and do it right now!)

For that reason, 23andMe refused to admit fault, which a company spokesperson rather bluntly stated in a letter to the affected customers: "users negligently recycled and failed to update their passwords following these past security incidents, which are unrelated to 23andMe. Therefore, the incident was not a result of 23andMe's alleged failure to maintain reasonable security measures."[99] In other words, the company took no responsibility for ensuring that user account credentials were reasonably secure. Two-factor authentication was available to 23andMe users, but was not required at the time (that has changed as a result of the breach; users are now required to set up MFA).

---

[99] *https://techcrunch.com/2024/01/03/23andme-tells-victims-its-their-fault-that-their-data-was-breached/*

The court cases are, as of this writing, still in litigation. Preliminarily I can say that I don't agree that the stolen information couldn't be "used for pecuniary harm" – it could easily be used to create highly-targeted phishing scams – and the initial grouping of stolen data into subsets of Jews and Chinese was certainly intended to enable hate groups, terrorist organizations, and autocratic regimes to target those people in specific, not just with phishing scams, but with extortion and physical harm. I also don't agree that 23andMe was completely innocent; surely the company's engineers and security experts knew that accounts could be compromised in this way, and consciously chose not to require strong passwords and MFA methods despite the fact that the service already had MFA capabilities. (This is why I urged you to enable MFA whenever and wherever possible in Chapter 1.)

Consider for a moment how 14,000 compromised accounts led to 6.9 million user records to be exposed to hackers. This was only possible because every one of those people opted-into the "DNA Relatives" feature, which automatically shares profile and some DNA data with other users who may be related to them. Had they simply chosen not to share their information, their profiles would not have been scraped and put up for sale on the Dark Web. Again, I urge you not to enable or opt-in to any sharing features of any of these DNA testing or ancestry tracing services; even if you keep your account secure, your personal information can be stolen by association and used against you in a variety of ways.

How Is It Collected?

Most **raw data** (human-comprehendible personal details such as your name, date of birth, and annual income) is collected directly from people in three ways:

1. **Freely offering it** through voluntary methods (or neglecting to take precautions to prevent it from being collected or shared).
2. **Passively** by way of methods that you cannot control, such as your mortgage lender sharing payment data with consumer credit agencies.
3. **Compulsively**, by being required by laws or user agreements to provide it.

Beyond that, algorithms create **calculated data** about us based on the aggregate of raw data that they're given. The most common example of calculated data is your consumer credit score (whether that be from FICO, TransUnion, or other credit agencies), but advertising platforms such as those owned by Google and Meta will also combine multiple data sources (such as your clicks, search history, and the amount of time you spend using an app or service) to create marketing profiles for you and multiple cohorts of people who have certain details in common. Then they use that data for their benefit, always at your expense.

While you can choose not to apply for a passport or driver's license (which compels you to provide accurate personal and private information to a state or national government) or a mortgage or credit card (which compels you to provide even more private information to financial companies), in general you can't stop government agencies and corporations from collecting at least some information about you (and in many instances it isn't worth the effort to try – do you really want to go without the privilege of driving a car or travelling overseas?). Neither can you legally stop someone from recording your public activities (unless it qualifies as stalking, but that's a different matter). It is impossible in the modern world (and even in previous paper-driven eras) to maintain 100% privacy, but as I explain in detail in Chapters 4 and 5, the more you protect your information (and the more of it you protect), the better-off you are.

Since the first volley of data breaches made national and international news headlines many years ago, a growing number of people have become more conscious of protecting their digital privacy. Because personal data is critical to those who collect and/or monetize it, all manner of data collectors have constantly found new ways to extract it from us.

Police Interaction

Cops can take notes specific to people, cars, or physical locations involved in calls, even if no crime has occurred. If the police visit your house or you talk to them about anything, everything you say and everything they observe will be recorded in a police database. If it's recorded in a municipal or state database, that information will likely be pulled into the FBI's National Crime and Information Center at some point.[100]

[100] *https://www.ojp.gov/ncjrs/virtual-library/abstracts/crime-scene-note-taking*

US federal law prohibits the police from accessing non-public information in these databases unless it is relevant to an investigation that they're involved with. (Well, *technically* it prohibits "unauthorized access to a protected computer," but it's the same principle). That doesn't mean that police officers don't perform unauthorized searches of law enforcement records. In fact they get busted for it all the time, and it's likely that many more aren't being caught because it's difficult to audit search records for databases that have millions of queries per day. Cops have been caught using government databases to illegally search for details about current or former romantic partners, neighbors, business associates, friends, enemies, celebrities, and even other cops.[101]

In most states, applying for a concealed weapon permit requires voluntarily giving identifying personal information (including fingerprints) to a local police department and the FBI. Depending on which state you're in, you may also be required to register all of your firearms with the state Department of Justice or with your local police department, which typically includes recording a description of the weapon and its serial number.

Push Notifications

Whenever a mobile app receives a push notification, the location of your device and any unencrypted information contained in the notification (such as the content of an email or text message) is visible to, and can be recorded by, the company that provides the app and the operating system. Even if you use an app that doesn't require you to identify yourself and encrypts your messages, the push notifications may still reveal significant information about you and your whereabouts.

Both the US and foreign governments have requested push notification data and metadata from Alphabet and Apple for various reasons.[102] Unless you're a spy or a criminal, you probably don't have to worry too much about this, but you should be aware of it nonetheless.

101

https://duckduckgo.com/?q=police+officer+caught+using+database&t=newext&atb=v237-1&ia=web

102 https://www.reuters.com/technology/cybersecurity/governments-spying-apple-google-users-through-push-notifications-us-senator-2023-12-06/

Card Skimmers and Hidden Cameras

Prior to chip-and-pin security measures, credit and debit cards were shockingly easy to counterfeit. All a thief had to do was record the card number, expiration date, and three- or four-digit code printed on the card (some or all of which could be obtained from a discarded receipt, invoice, or statement), and he or she could press a fake card and write the necessary data to the magnetic stripe. The tools required for this operation are not illegal, and can be acquired for less than $200.

As of the publication of this book, all credit and debit cards now have integrated microchips that are much more difficult and expensive to clone. This can prevent a large amount of credit card fraud at physical points of sale, but only if the card reader exclusively accepts chipped cards; many point-of-sale devices don't have chip readers at all, or offer a magnetic stripe reader as an alternative. Thus, cloning a credit card without a chip is still a viable technique.[103]

Thieves don't need to go **dumpster-diving** (looking for cards and documents containing critical personal or financial information in people's trash) anymore to get credit card numbers, though. They can obtain credit card details from one of the multitude of e-commerce data breach caches available on the Dark Web, but much of that data is old – those cards have been cancelled. The quickest and easiest way to clandestinely obtain a fresh set of all of the information required to create a counterfeit credit card is to use a **card skimmer**: a small device that reads and records the data on a card's magnetic stripe.

Card skimmers can be isolated devices that a clerk, bartender, or waitress will use in addition to a legitimate point-of-sale device when you hand them your card to make a purchase. At some point in the future, they will either use that skimmed data themselves or give or sell it to a professional thief. More commonly, though, card skimmers are designed to subtly attach to legitimate point-of-sale devices. A thief secretly adheres the skimmer to the face of the card reader, then comes back later to retrieve it. Crude skimmers are obvious upon inspection (an extrusion glued or taped onto the end of the stripe reader of a point-of-sale device), but are often ignored anyway. The most advanced skimmers are so cleverly

[103] *https://finance.yahoo.com/news/chip-cards-counterfeit-proof-not-120054469.html*

engineered that they cannot be detected at a glance; they are custom-designed to match the exact materials and colors of the point-of-sale device. Fortunately they have one critical fundamental flaw that makes them easy to discover: they are designed to be quickly applied and removed, and therefore will detach if you pull at them.

You may be wondering what the benefit of skimming a debit or ATM card is, since they require secret PINs that are not printed on the card or stored on the magnetic stripe. To steal your PIN, thieves will install hidden cameras pointed at the PIN entry pad, or their card skimmers will include a veneer for the keypad that also records button-presses. Keypad veneers are, like stripe skimmers, designed to be quickly removed, so you can test for them by tugging on the keypad and the surface around it. Hidden cameras are very difficult to find, but you can defeat them by covering your PIN entry with your other hand or an object such as a hat or handkerchief.

Credit and debit cards aren't the only things worth stealing; your driver's license, work badge, and anything else with a magnetic stripe can also be swiped by a skimmer and counterfeited.[104] Scanning or photographing driver's licenses is now a standard practice at many hospitals, liquor stores, and even supermarkets. State laws vary wildly as to whether, when, and by whom a state-issued ID can be scanned, whether and how long scanned ID data can be stored, and if and how it can be used for other purposes beyond verifying age or identification.[105] While many states prohibit scanning IDs for purposes other than age verification (such as when buying alcohol, tobacco, or pornography) and other legally-sanctioned reasons, when ostensibly used for "security purposes," companies are generally allowed to be opaque about their information collection and usage practices. Even if the company doesn't retain swiped identification data, just like with credit cards, the people doing the license-swiping may be illegally double-swiping people's IDs with their own black-market skimmers.

Vigilance and skepticism are two of the most important tools in protecting your information. Stealing information from people's driver's licenses, work badges, and credit cards can be as simple as asking them to hand over their cards to be swiped. A thief dressed as a security guard could stand

---

[104] https://www.nbcmiami.com/news/local/security-experts-beware-of-companies-scanning-your-drivers-license/156850/
[105] https://idscan.net/us-id-scanning-laws/

outside your work building and say that the badge sensor isn't working, so he has to scan your work badge with his own device. Someone wearing a polo shirt that says "SECURITY" on it could ask to swipe people's IDs in a stadium or theater concourse. Someone dressed like a server or bartender could walk up to people in a club and ask them to prove that they're of legal age to drink. It isn't inherently illegal to own or wear clothing that fits these descriptions. (It is, however, extremely illegal to pretend to be a law enforcement officer; that doesn't mean that criminals don't try to get away with it.)

It's perfectly okay to give these kinds of people the third degree before handing over your cards or credentials. You have no easy and reliable way of knowing if someone is who they (or their costume) say they are; this could be a legitimate member of security staff, or it could be a thief dressed like one. If you're confronted to present your ID in a place where there are law enforcement officers present – such as a concert or football game – it's okay to ask the officer if this is a legitimate security guard, and if you're under an obligation to hand over your ID to be scanned. If it's just a lone security guard standing outside the building, ask for another member of the security staff to come out and verify that you should be handing your ID to this person. Good security personnel should be aware of these issues and be eager to support your desire to ensure that proper procedures are being followed, and should have no problem complying with your request. Not all security personnel are good at their job, though.

Hidden cameras can also have nefarious utility outside of recording debit card PINs. They can record access code entries for doors and garages, hiding places for keys, screen lock codes for mobile devices, and passwords (when typed).

In summary, here are some actions you should take:

- Never use a debit card for anything other than an ATM transaction, if possible. If your credit card is counterfeited, you can quickly call the bank and have the fraudulent charges reversed and your card replaced. If your debit card is cloned, you will lose cash from your checking account; you can still get it returned through the same process if you respond quickly, but if you incur fees (for using the ATM, overdrafting the account, or bouncing a check) the bank is likely to fight you on at least some of them. Banks make a lot of money from fees.

- Whenever possible, never give any of your cards (ID, credit, debit, etc.) to someone to swipe outside of your supervision. Obviously you must give your driver's license to law enforcement upon request, but no one else should ever need to take it out of your sight. This is very difficult to do in most restaurants, unfortunately, because credit cards are usually processed at a register or server stand. You might consider only using one specific credit card for restaurants, to limit your exposure to potential fraud.

- Before you insert a card into a reader, inspect it for extrusions or anything that looks like it isn't supposed to be part of the device. Tug on the card reader slot to see if it comes loose (don't worry, you won't break it), and if there's a PIN pad, tug at and around that too.

- Never enter a PIN, code, or password in public (or in public view) without covering your hand such that your keypresses cannot be recorded if there's a camera pointed at it. You might also consider doing some dummy keypresses (act like you're pressing a button, but don't actually push it) before and after your PIN so that even if the sequence is recorded on video, the true code or PIN will be difficult to determine.

- If your bank offers a service to notify you of all card transactions via mobile app, text message, or email, enable it. Be wary, though: thieves have been known to send fake text messages pretending to be your bank notifying you of a false charge. If you get a text message or email like this, do not respond to it or use the contact information provided in it! Instead, call the number printed on your card.

- Examine every purchase on your statement before you pay it. If there are any unfamiliar transactions, call your bank immediately (or if you share a card with a family member, check with them first; also consider the fact that some businesses process credit card transactions under a slightly different corporate name or via a processor like Square).

- Be suspicious of anyone who isn't a police officer asking you for your ID or other swipeable credentials. Wearing a costume is not proof of authority.

Stalkerware and Physical Trackers

The US Federal Trade Commission defines **stalkerware** as any app or service that secretly tracks or monitors a person through their mobile device.[106] Modern stalkerware can enable an abusive romantic partner or ex-partner to monitor and record:

- Your device's current and previous locations
- Incoming and outgoing voice calls, text messages, multimedia messages, and email
- Photos and videos recorded, sent, or received
- Online activity, including social media, Web search, and website history
- Anything your device's camera can see and/or its microphone can hear

Being an Apple fan won't help much; the Apple App Store may have stalkerware in it at any given time, and Apple even sells Airtag devices that allow someone to secretly track anyone or anything they're attached to. In general any app or device that is designed for location-tracking can be used for stalking purposes. Often these apps are presented in the context of helping parents keep track of their children, or to help find a lost mobile device. While they are usually useful for those purposes, unfortunately, as I detail in the "Stalking, Social Catastrophe, and Suicide" section of Chapter 4, these apps can also be used by stalkers and predators to track their victims.

In addition to Apple Airtags, there are many kinds of keychain-sized "smart tags" on the market from other manufacturers that can be placed on or in something such as a purse, suitcase, or car, that enables the owner to track its location. This is handy for finding lost luggage or a stolen purse, but it's also useful for secretly stalking someone. If you believe that someone may be stalking you, in addition to notifying the police, you should empty your bags and search your vehicle for these kinds of tracking tags.

[106] *https://consumer.ftc.gov/articles/stalkerware-what-know*

Trickery Through Digital Dark Patterns

A **digital dark pattern** is a software design decision that encourages people to unintentionally perform an unwanted action that costs them time, money, or otherwise coerces them into doing something that they did not consciously agree to, for instance: clicking on an ad; sharing information that isn't required to use a service; or spending money impulsively, mistakenly, or in the case of minor children, without their parents' consent. Here are the most common digital dark patterns, as provided by the US Federal Trade Commission:[107]

- **Design elements that cause false beliefs.** For example, when marketers use deceptive **masquer-ads** that look like independent editorial content, but actually are paid content or advertising; or when an ad says "DOWNLOAD NOW" on a webpage where you intend to download something else.

- **Design elements that hide key information.** This category includes the practice of burying additional fees, mandatory charges, or **drip pricing** (also referred to as **partitioned pricing**, **shrouded pricing**, and **"nickel-and-diming,"** where the advertised price is considerably lower than the final sale price due to hidden fees and mandatory charges) in hard-to-find or even harder-to-understand blocks of text, often late in the transaction.

- **Design elements that lead to unauthorized charges.** Marketers who take advantage of these dark patterns typically trick people into paying for goods or services they didn't want and then bill them – often on a recurring basis – without their consent.

- **Design elements that trick customers into sharing personal data.** These dark patterns often appear to give consumers a choice about sharing data, but then cleverly steer them to the option that enables them to collect personal information.

[107] *https://www.ftc.gov/business-guidance/blog/2022/09/ftc-issues-illuminating-report-digital-dark-patterns*

Here are some specific examples of those patterns:[108][109][110]

- **Confirm-shaming**: when a service, site, or app pesters you with extra confirmations (usually with emotional cues) after you've opted-out of something you don't want. For instance if Amazon pushes you to sign up for its Amazon Prime service, then forces you to click a button that says "No thanks, I don't want Unlimited One-Day Delivery." Online games might show one of its characters looking sad or defeated if a user refuses to purchase an add-on or cancels a subscription.

- **Grinding**: rewarding a repetitive action or series of simple tasks, especially in a video game, that requires an investment of time (or simply the act of logging into the service) instead of proof of a skill.

- **Pay-to-win**: giving users an in-game advantage or extra social prestige for paying extra.

- **Waste aversion**: threatening to erase or delete a user's achievements, scores, characters, digital currency, or other content if they cancel the service.

- **Comparison prevention**: making it difficult for people to compare and contrast the features of different products or levels of service.

- **False scarcity**: lying about the limited availability of a product or service (such as a plane ticket, hotel room, or physical product inventory) to inspire a sense of urgency and "the fear of missing out."

- **False urgency**: similar to false scarcity, the site or app displays a countdown timer that requires them to complete a purchase within the given interval.

---

[108] https://lawreview.colorado.edu/printed/when-the-cats-away-techlash-loot-boxes-and-regulating-dark-patterns-in-the-video-game-industrys-monetization-strategies/
[109] https://www.deceptive.design/types
[110] https://perma.cc/S32Y-7N8F

- **False social proof**: publishing fake reviews, testimonials, or activity notifications, especially from people who ostensibly share things in common with the user or visitor (such as their location as determined by their IP address, or other personal details that can be gleaned from a third-party cookie or other data-sharing scheme).

- **Friend spam**: when you are pestered to sign up for a service or download an app (via email, text, mobile notification, social media, or other means) because someone you know has done the same.

And here's how those patterns most often manifest in mobile apps, websites, and online games:

- Making it easy to mis-click or mis-tap an interface element that immediately executes an unwanted purchase, vote, or other act of consent without further confirmation or ability to cancel.

- Altering the document model of a website so that the links or buttons shift position after a user clicks on one, thereby forcing him or her to unintentionally click on something else.

- Putting an obtrusive ad on the screen, and making the close (X) button inoperable or too small to reliably click or tap on, causing unwanted engagement with the ad's content.

- Switching button-click paradigms in successive window elements so that (for instance) "cancel" and "ok" are reversed from their previous orientation.

- Refusing to refund mistaken purchases, and/or punishing users by revoking their access to the entire app / site / game when they request a refund for an optional add-on purchase.

- Requiring a high level of effort to cancel a subscription service that users were automatically and unknowingly subscribed to.

- Currency conversion incongruity in services that require purchases to be made in a special digital currency that does not convert from real money in a way that ends in even numbers. For instance an in-game item might cost 1100 tokens, but users can only buy tokens in blocks of 1000.

- Mixing required consent checkboxes (for instance: software license agreements, user access agreements, and privacy policies) with optional consent checkboxes (usually granting permission to collect and/or share your data with "partners" or add you to a mailing list).

Case Study: How Fortnite Harmed Kids and Overcharged Adults

Late in 2022, the US FTC settled two complaints against Epic Games pertaining to its wildly popular battle royale game *Fortnite*, totaling a record-setting $520 million.[111] That may seem like a lot of money until you consider that Fortnite has earned multiple billions of dollars – $9 billion in revenue in its first two years alone, and as of the publication of this book, the game's been around for more than six years.[112] The complaints credibly accused Epic of using digital dark patterns to make it easy for adult players to make accidental purchases, to punish players who disputed unexpected charges, to encourage children to make unauthorized in-game purchases, and to illegally expose kids to voice and text communication from strangers (a violation of the Children's Online Privacy Protection Act, or COPPA).[113]

The first FTC complaint showed that Epic set up its payment system and user interface to make accidental or unauthorized purchases easily, with no way to reverse or refund them. Primarily these purchases were for virtual in-game currency called V-Bucks (another digital dark pattern, as explained earlier in this section), which players then used to buy in-game items. Parents who had authorized their kids to make a one-time purchase with their credit card found that their kids had – intentionally or accidentally – racked up hundreds of dollars of additional V-Bucks charges. The Epic employee in charge of risk management and fraud recommended that the company require inputting the credit card's CVV number as a method of validating the purchase (which would prevent kids from charging their

[111] *https://www.ftc.gov/business-guidance/blog/2022/12/245-million-ftc-settlement-alleges-fortnite-owner-epic-games-used-digital-dark-patterns-charge*
[112] *https://www.theverge.com/2021/5/3/22417447/fortnite-revenue-9-billion-epic-games-apple-antitrust-case*
[113] *https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-are-latest-battle-royale-against-violations*

parents' card unless they were in physical possession of it, and would allow adult players a chance to cancel an accidental purchase), but his advice went unheeded until the problem had become large enough to attract the FTC's attention.

Fortnite's interface was designed to make accidental purchases easy by mis-clicking or mis-tapping on buttons that the player thought would allow them to preview a cosmetic item before committing to purchasing it. Users also reported that *Fortnite* would occasionally make unintended purchases on its own by pre-registering taps or clicks during loading screens or when the device was waking up from sleep mode. On consoles, *Fortnite's* interface switched the buttons for previewing and purchasing in different screens. Over the course of four years, Epic received more than a million complaints from its users about unauthorized or accidental purchases, refunds for which were largely not honored. When customers went to their credit card companies to dispute the charges, Epic locked them out of their *Fortnite* accounts, and prevented them from using not only the items that were accidentally purchased, but also everything that they'd intentionally bought in the past. The FTC required Epic to use the $245 million civil penalty to issue refunds to customers who'd made V-Bucks purchases.

The second complaint holds Epic responsible for designing *Fortnite* to appeal to underage players, and collecting personal information about them without parental consent. The FTC determined Epic's intent from surveys that showed that 86% of US children aged 10-17 played *Fortnite* on at least a weekly basis, and from statements made by the game's developers, such as: "We want to be living room safe, but barely. We don't want your mom to love the game – just accept it compared to alternatives." Despite that and several other employee statements supporting Epic's desire to appeal to underage players, *Fortnite's* lengthy privacy policy explicitly stated that the game was not directed at children.

Fortnite launched without any parental control features (despite this being a widespread industry practice at the time), and offered few privacy settings. It also enabled unfiltered voice chat by default, and its multiplayer algorithms did not take players' age into consideration; as a result, children were put onto teams with adults, with voice chat enabled. The FTC documented several examples of children being threatened, bullied, sexually harassed, asked for sexually-explicit photos, and exposed to traumatizing encounters involving self-harm and suicide, all by way of *Fortnite's* on-by-default voice chat.

In 2019, Epic put an "age gate" in place to try to prevent kids from signing up for *Fortnite* (which is free to play, but contains many options for in-game purchases) without permission from their parents, but it did not attempt to apply it to existing accounts. As part of the settlement, the FTC prohibited Epic from enabling voice and text communication by default for kids unless they had parental consent, and to delete all personal information it had collected from underage users.

"Free" Things

Back in Chapter 2 I encouraged you to migrate away from "free" services because most of them fundamentally violate your privacy. With few exceptions, they collect personal information about you, then use that to target you with ads everywhere you go.

There's another kind of "free" that you should be wary of, though: the "free gift." The very concept of a "free gift" is silly because gifts, by definition, are always free for the recipient. Marketers like to emphasize the word "free" whenever possible, though (often in capital letters), because it gets people's attention, and while the "gift" may be free of upfront monetary cost, you'll end up paying for it in some other way.

The old maxim "There's no such thing as a free lunch" is not true in the literal sense. For instance many corporations offer catered lunch as a universal perk for all employees, and soup kitchens and food banks exist to offer the poor and homeless a no-strings-attached meal for free. Of course there are fundamental costs involved behind the scenes, but they aren't paid by the person receiving the meal. Metaphorically this phrase is fundamentally true, though; if you get something of value for free from a corporation, then you're paying for it indirectly, either with money spent on something peripheral, or with something else of value such as your time, attention, or personal information. <u>If you're not the customer, then you're the product.</u>

Traditionally the currency you trade for a "free" item or service is your contact and/or demographic information, which will later be used to send you junk mail, spam, and unwanted calls and text messages from salespeople. Marketers have always offered "free gifts" to generate sales leads because, in aggregate and on average, whatever "gift" is being offered for "free" is objectively less valuable than a qualified sales lead. One of the most well-known and longstanding examples of this practice is when

timeshare companies offer "free" tickets to amusement parks in exchange for as much of your personal information as possible and a commitment to sitting through their hours-long sales pitch. If you decline to buy the timeshare (or even if you don't), you can count on being spammed with timeshare deals (and probably other vacation-related services as well, depending on who the timeshare company sells your data to) far into the future.

Browser History and Web Trackers

Nearly every website you visit, every mobile app you use, and even many of the emails you receive contain hidden tracking code that reports a variety of personal information back to as many as a dozen or more analytics service providers or data brokers. Mostly this data is used for understanding user activity, but when the company that owns the site or sends the email already knows who you are, then it can combine that tracking information with other data it's already collected about you. That will, of course, be used to tailor ads and other marketing materials for you as specifically as possible.

As I explained in Chapter 2, most tracking code can be blocked by using privacy-focused Web browsers and email services, and by using a VPN.

Corporate Partnerships and Data Sharing

Nearly every modern corporation and non-profit organization collects information about customers, users, clients, members, or donors, and uses it to solicit them in the future through a variety of methods. Many of them also purchase information from data brokers, and some (especially technology companies) sell data to data brokers or share it with other companies, contractors, or vendors that they have a business relationship with ("partners").

Beyond that, there are some grey areas where companies share data indirectly. For instance Google Ads allows advertisers to upload customer data to create specific audience groups; Google uses this data in combination with its own personal data hoard to target every person in that customer list with ads.[114] Alphabet doesn't make judgements about the

[114] *https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and*

data its Ads customers upload; it could be an exported list from an internal **CRM** (customer relationship manager; software that helps businesses record, organize, and track personal data collected from customers or sales leads), or it could be a list purchased from a data broker or the Dark Web.[115] If one of the people on that list clicks on the ad that was targeted at them, the landing page will almost certainly contain tracking code that will match up with the information provided by the company, which now has a layer of metadata applied to it by Google Ads. Companies can then use this refined data to get more specific with their ad targeting. For example a sportswear retailer might purchase a list of millions of NFL fans from a data broker, upload it to Google Ads, then create a unique ad that is designed to appeal to female Green Bay Packers fans, and blast it out to the Internet. Google will only show that ad to the people who are on the list. If 50,000 people click on the ad, then the tracking code embedded in the sportswear store's landing page will attempt to match them with the original list of football fans, resulting in a refined list of female Green Bay Packers fans and whatever personal information has been collected about them along the way.

While Alphabet claims that it does not directly sell personal data ala a traditional data broker, it does make quite a bit of its user data available to Google Ads customers.[116] Ostensibly this is supposed to be used only for ad targeting, but there are ways for customers to "siphon off" that data to use for other purposes.[117] A group of Google users exposed this practice and filed a lawsuit against Alphabet in US District Court in San Jose, CA in May of 2021.[118] As of the publication of this book, the lawsuit is still pending.

Alphabet is by no means the only company that does things like this. Meta also makes customer data available to its advertisers in a similar indirect

---

115 https://support.google.com/google-ads/answer/6379332?hl=en

116 https://ecf.cand.uscourts.gov/cgi-bin/DktRpt.pl?778966527788442-L_1_0-1

117 https://www.mercurynews.com/2021/05/07/google-selling-users-personal-data-despite-promise-federal-court-lawsuit-claims/

118 https://www.cpmlegal.com/news-Lawsuit-Seeks-to-Stop-Google-from-Secretly-Selling-Americans-Private-Information-Without-Informed-Consent

manner, and has been caught making Facebook user data available to outside marketing firms.[119]

Trojan Horses (Legal)

The original Trojan Horse is documented in Homer's *The Iliad:* unable to breach the defenses of the city of Troy, a group of Greek soldiers hid inside a huge wooden statue of a horse, and a few of their compatriots hauled it up to the gates of the city, ostensibly offering it to their enemies as a "free gift." When the Trojans brought the statue inside the city walls, Greek soldiers emerged from it and sacked the city. In the modern world, **trojan horses** traditionally refer to any software or device that pretends to be helpful or benign, but actually serves a harmful purpose. It's useful, for security and privacy purposes, to expand that definition to include processes, services, and activities as well. (I differentiate between *legal* and *illegal* trojan horses; the illegal variety is covered later in this chapter in the "Methods of Intrusion" section).

For instance a classic method of collecting personal information from people is to host a contest or giveaway that offers a prize via a random drawing. Participants are required to provide their name, contact information, and other details in order to enter the drawing. This is perfectly legal so long as the contest follows local and Federal regulations, and a winner is actually drawn and receives the prize unconditionally as promised. It isn't entirely honest, though; you believe you're only entering a contest, but the true motive is for a salesman or company to collect sales leads. Once you've handed over your information, you can expect to be spammed indefinitely through physical mail, email, text messages, social media, phone calls, and perhaps someone may even show up at your home to deliver a sales pitch in person. Your information may even be sold or shared with other salesmen or companies.

Some examples of legal trojan horses:

- Contests
- Lotteries (except the ones officially sponsored by a government)

---

119 *https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal*

- Giveaways
- Petitions (when they require more than just your name)
- Quizzes
- Polls (except when they don't require any personal information)
- Surveys
- Personality tests
- Job or volunteer applications
- Coupons and discount programs
- Warranty or product registrations
- Sign-ups of various kinds (such as to join a mailing list, to be notified of a new product release, or to tour a home for sale)

I encourage you not to participate in these kinds of things whenever they require handing over any of your personal information. Obviously if you're applying for a job, you'll have to provide at least some personal information, but whenever possible, do it on paper and in person or by phone. Applicant-tracking software is widely used by modern companies ostensibly to help qualify and track employment candidates, but you have no idea if your data will be kept for any length of time, if it will be end-to-end encrypted, and if it will be used for other purposes later. At very least, I advise you to be skeptical and cautious of such software, and never to input your social security number or bank account number. If the company's HR representative asks for your SSN in order to run a background check on you, ask them to explain in detail how that information will be handled, if it will be stored, when it will be deleted, and who will have access to it. And remember what you learned back in Chapter 2: fake job applications and publicly-posted resumes are a gold mine for identity thieves and scammers.

If all you need to provide to participate in something is your email address, then it's probably safe to provide a masked or anonymized email address as explained in Chapter 2. I also have some tips for providing alternative contact information in Chapter 6.

Data Breaches

In this book I use the term *data breach* broadly to encompass any incident in which personal data or secrets of any kind have been stolen, copied, exposed, released, or revealed by accident or through a criminal act. Security researchers sometimes like to define unique terms for specific types of incidents, but in my opinion it isn't useful to draw those distinctions here.

If you've passively scanned news headlines over the previous two decades, then you've at least accidentally read at least one article about a major data breach that exposed the personal information and/or login credentials of millions of people. In fact there have been thousands of such breaches over the years, and new ones frequently occur; in 2023 alone, there were more than 3200 data breaches impacting more than 350 million people.[120][121] Unfortunately no matter how careful you are in protecting your privacy, it's a certainty that at least some of your personal data has been leaked to the Dark Web via one or more data breaches in the past, and more will be exposed in future incidents.

Just because some pieces of personal information have already been exposed and/or collected doesn't mean you should give up trying to protect your privacy. A lot of the data that is stolen or collected becomes irrelevant within a short amount of time. For instance every time you change your phone number, physical address, bank, employer, relationship status, or any other meaningful aspect of your life, any data older than that becomes less useful to marketers and thieves. Old information can still be worth something in certain circumstances, though, such as when MFA security questions ask for "the street you grew up on" or your maiden name. This is why I encouraged you to use dummy information or secondary passwords for security questions in Chapter 2.

Information stolen in each data breach should always be assumed to be cumulative. If your full name and date of birth are stolen in a data breach at your *alma mater* University, and your Social Security number and current address are stolen from a ransomware attack (this is explained in detail in the "Methods of Intrusion" section later in this chapter) on your county government, and your email address and phone number are published on

---

[120] *https://www.idtheftcenter.org/publication/2023-data-breach-report/*
[121] *https://privacyrights.org/data-breaches*

a resume you posted online, then assume that all of this information is available to thieves even if these incidents happened years apart.

Throughout this book I provide several examples of notable data breaches, but it's impossible to cover them all and how they're executed. In the sections below, I explain generally how most data breaches happen, and who is most impacted by them.

Stolen Data is a Means, Not an End

Thieves, in general and by definition, are ultimately trying to take money or property from people, governments, and businesses. Sometimes this is direct and immediate – a mugging, burglary, or bank robbery, for instance – and sometimes it's a circuitous path involving multiple steps and a clever plan. While there can be some profit in selling caches of personal data on the Dark Web, more commonly the goal is to use personal data as part of a larger scheme to defraud or steal from victims. The one exception to this rule is espionage, where a three-letter agency steals personal data in order to identify spies and foreign agents.

When there are millions of stolen records to use, many thieves, fraudsters, and scammers won't target anyone in specific; instead they'll use a script that attempts to use each record for some kind of brute force attack (this is defined in the "Methods of Intrusion" section later in this chapter). For instance if you have a Yahoo Mail account that you haven't used in many years, you might think that it isn't terribly important if a hacker were to steal its login credentials, but that old email account isn't necessarily the target. Rather, hackers will hope that you reused the same username and password elsewhere, and create a program to automatically try those login credentials on a variety of other sites where purchases can be made, money or cryptocurrency can be sent, or a bigger collection of personal information can be stolen, such as Amazon.com, DropBox, or Coinbase, among many others. The ultimate goal is to break into one of these kinds of sites. When this automated method of attack is successful, the hacker will then get personally involved to figure out what can be stolen.

Less sophisticated thieves might simply start at the top of the list of stolen data – or pick one record at random, or search for names that suggest certain ethnicities – and try to use it for identity fraud or phishing scams (phishing is covered in detail later in this chapter in the "Methods of Intrusion" section).

Sometimes information is stolen solely for spam purposes. A valid Yahoo Mail, Gmail, or Discord account is extremely valuable to spammers and scammers because any messages they send from those accounts will appear to be legitimate to their contacts, and are therefore more likely to be seen and clicked-on.

Earlier in this chapter I listed the most dangerous kinds of personal data to reveal or share. That's primarily from an identity theft standpoint; low-level personal information is merely a stepping stone to a larger theft. Ultimately cyber-criminals are looking for these things:

- Cryptocurrency wallet recovery phrases
- Email login credentials
- Gift card redemption codes
- Bank account numbers
- Credit card details (including the CVV code and expiration date)

If you're surprised to see "email login credentials" in that list, then I encourage you to consider what's archived in your email account. You could have a treasure trove of secret information there, not just in email but in attachments: full Federal tax returns, bank statements, nude photos, login credentials for various things, and gift card codes. In fact there are thieves who specialize in silently breaking into people's email accounts simply to search for – and steal – gift card codes; victims have no knowledge of these thefts until they try to use those codes, which could be months after they were received via email.[122] Email is also a popular destination for 2FA codes and password reset links; by gaining access to your email account, a thief could reset your passwords on various sites and services.

Speaking of gift card codes, thieves will also look for retail gift card racks in stores and record the codes from them. Those codes aren't yet activated, but at some point they will be (after someone buys one and activates it at checkout), so it's just a matter of periodically brute-forcing all of the codes they've collected. Chances are pretty good that they'll get to the gift card

---

[122] https://krebsonsecurity.com/2021/09/gift-card-gang-extracts-cash-from-100k-inboxes-daily/

balance before the legitimate recipient has the chance to use it. So if you purchase a physical gift card, make sure that its redemption code is not visible prior to the sale, and encourage the recipient to use it as soon as possible.

High-Value Targets

Some thieves specialize in targeting specific types of victims, and will search and sort through stolen data to identify them:

- **Wealthy people**. For obvious reasons it's worth the extra effort for criminals to try to collect personal data on people who are known to be wealthy. While the rich typically have a higher level of physical security – especially at their home(s) – they are vulnerable to highly-targeted phishing scams (often referred to as **spear phishing**), extortion, and embezzlement, especially if they entrust their finances to assistants and accountants.

- **Lottery winners**. These people are particularly vulnerable to thieves because their name and the amount of their windfall is widely published, and they nearly always live in middle-class homes or apartments that are easily burglarized (whereas people who have long-term wealth tend to live in upper-class housing with high-end security measures).[123] Beyond traditional physical robbery, lottery winners are susceptible to the same spear phishing scams as wealthy people.

- **Famous people.** People who are famous are not necessarily wealthy, but they are generally assumed to be. Even when they are known not to be particularly wealthy, famous people are often a high-value target for trolls, stalkers, and terrorists, who use many of the same tools as thieves and scammers. Fame intrinsically erodes a person's privacy, which makes it easy for attackers to collect and use all manner of personal information – particularly where they live and work, and their whereabouts at any given time. Professional athletes are frequent targets of home invasion robberies because thieves know that they won't be home when they're competing in a match.

[123] *https://www.nbcnews.com/id/wbna6066353*

- **The elderly**. Scammers love the elderly for many reasons: they often have money to steal, they grew up in an era before phone scams and phishing and aren't aware of such things, and sometimes they suffer from dementia and are easily convinced that they're talking to an old friend or family member.

- **The infirm**. When someone is hospitalized for a length of time, thieves know that there's a good chance no one's home, so it's relatively safe to break in and steal their things. Savvier thieves will steal the victim's mail as well (which may contain bank statements and "get well" cards with cash, cheques, or gift cards enclosed), since it probably is piling up in the mailbox. If someone you know is going into the hospital for a procedure that will keep them away from home for more than a day, you can help by offering to house-sit and pick up their mail for them.

- **Dead people**. No one is more vulnerable to theft than the deceased. Unfortunately, stealing from the departed is not a victimless crime; their next-of-kin are entitled to their inheritance, and sometimes also Social Security money, pension payments, and health care benefits. Even if there's no next of kin, that money still legitimately belongs to someone, even if it's the Federal government (which is funded from the taxes that we all pay) or a corporate pension fund (which workers have paid into with their labor). When someone close to you dies, it's critical that the legal paperwork be processed as quickly as possible. Thieves read obituaries and will try to steal the identity of the deceased and obtain credit, prescription drugs, and/or Social Security benefits in their name. If the government (via the local Department of Health and the Federal Social Security Administration) does not know someone is deceased (by way of a death certificate), then that person's Social Security number will still be valid long into the future. Typically a licensed funeral director will assist with this process, but it's a good idea to make sure they follow through with it. Also, as with people who are hospitalized, thieves know that there's a good chance no one's home at the deceased's residence, which makes it a prime target for burglary.

- **Anyone who could reasonably be a hacking target**. If you're a politician, social activist, or an executive at a company or in an

industry that attracts negative attention (oil and gas, pharmaceuticals, health insurance, hedge funds, religious institutions, political organizations, etc.), then you can expect that you'll be more of a target for hackers, trolls, and terrorists.

Among potential institutional targets, these are the most at risk:

- **Federal government agencies**. Foreign intelligence agents – particularly from Russia and China, but sometimes even from countries that are allied with the United States – are constantly trying to break into Federal government databases. Primarily they seem to be looking for information on spies, but they are of course also interested in any information related to military deployments and capabilities.

- **Local governments and infrastructure (utilities)**. Local governments and utilities are a prime target for ransomware attacks because they usually pay the ransom and they often use vastly outdated computer systems that are full of security flaws, but sometimes foreign agents are more interested in simply disrupting infrastructure services to cause chaos and economic harm.

- **Companies that produce cutting-edge technology, especially if it's export-restricted**. Chinese military intelligence is particularly interested in stealing trade secrets that can be used for military purposes. This doesn't just apply to defense contractors; a surprisingly wide array of commercial components and products are used in, and are useful for, military applications. Any cutting-edge technology developed in the US is a prime target for industrial espionage; even if it has no military purpose, it can be copied and used by Chinese companies to produce consumer goods. The FBI estimates the value of those stolen secrets to be between $200-$600 billion annually.[124]

- **Companies that produce or provide information security-related products and services.** For obvious reasons, predatory hackers and foreign agents are highly interested in compromising Western companies that manufacture devices or provide services

[124] *https://www.businessinsider.com/recent-spy-case-shows-how-industrial-espionage-helps-chinese-military-2021-12?op=1*

related to information security: firewalls, VPNs, password management services, operating systems, servers, routers, strong encryption chips and algorithms, and authorization and authentication platforms.

Don't Ignore Small Breaches

High-profile data breaches usually involve carefully-planned long-term efforts to hack into a large government database or corporate server, but I want you to broaden the concept of *data breaches* to include any unauthorized disclosure of personal information, even if it was accidental, and even if you were the only victim. For instance:

- A radiologist mistakenly sends your MRI images to the wrong doctor
- Your child's school grades are sent to a different student
- A detailed invoice or bill for goods or services is mailed to the wrong address
- Your church publishes a list of every member's full name, address, phone number, email address, and date of birth
- A bug in a social media app makes your entire profile public for a few hours
- A Reddit troll uses clues in your comment history to **dox** you (publish personal information with the intention of causing you serious harm, most notably your home address, school or employer, and phone number)
- An anti-abortion activist publishes a list of patients of a local Planned Parenthood office

Many of these kinds of small-time data breaches aren't going to lead to any kind of harm, but the fact that they happened means that the people in charge of safeguarding your personal information have violated their duty. A doctor mishandling your records or radiological imaging is just as much a violation of your privacy as the massive Equifax breach of 2017. Not only that, it's also in violation of Federal HIPAA regulations. I encourage

you to hold people – and especially corporations – accountable when they are careless with your personal information.

Any kind of school, small business, religious organization, non-profit, or local utility provider is potentially vulnerable to a small-time data breach with a potentially big-time impact on a relatively limited group of victims. It's impossible to say how many of these there have been because they don't usually get reported, but I think it's probably a very high number, and even though only a handful of people may have been impacted by each one, in aggregate they likely add up to hundreds of millions of people.[125]

Methods of Intrusion

So far in this chapter I've covered the kinds of personal information that is legally collected about you, who is collecting it, and why it's so valuable to them. In the subsections below, I'll explain how that data is stolen – both from individuals and organizations.

Brute Force

A **brute force** attack is when a thief uses automation (such as a computer program or phone auto-dialer) to make repeated attempts to gain access to someone's account. Examples include (but are not limited to):

- **Dictionary attacks**: When a hacker knows your username but not your password, they can use a database of potential passwords to try to guess it through repeated login attempts. Long ago hackers would use a list of dictionary words, since people often choose a password they can easily remember. In modern times they also use lists of names, numbers, and dictionary words that have one or more letters replaced with a number or symbol.

- **Credential stuffing**: Similar to a dictionary attack, except the hacker will use a database of stolen login credentials to attempt to access other accounts, hoping that the victims reused their usernames and passwords across multiple services.

[125] *https://www.consumerreports.org/electronics/data-theft/the-data-breach-next-door-a7102554918/*

- **Cracking weak encryption**: When personal information – login credentials in particular – are encrypted using very old and weak methods, hackers can use programs to try to break the encryption.

- **2FA fatigue**: Intentionally triggering two-factor authentication notifications via mobile app, text message, or email with the hope that victims will blindly approve it. This also encompasses false 2FA requests, such as sending a text message to the victim asking them to reply with a 2FA code from an authenticator app.[126] Enabling MFA everywhere – as I encouraged you to do in Chapter 2 – does have a downside: you'll have to go through the MFA routine every time you log into an app or website, which you can become annoyed by or numb to after a while. Remember to pay close attention to every MFA request and notification, and don't approve it if you aren't 100% sure that you requested it.

In terms of data breaches, hackers will use brute force techniques with administrator or root user accounts to log into servers that store unencrypted personal data. By logging into a server with admin credentials (or by logging into a router or other intermediary device or service where unencrypted network traffic can be intercepted), the attacker can copy any unencrypted data stored on it (or, if the admin account has the encryption keys, they can decrypt the data and then copy it), and/or install malware that will enable them to steal more data in the future. In **ransomware** attacks, the hacker will encrypt all of the data on the server using his own key, then demand payment in exchange for the encryption key.

Phishing and Social Engineering

Phishing is any method of obtaining personal information through deception; it is a subset of **social engineering**, which is the process of psychologically manipulating others into performing actions that they would ordinarily refuse to do. The vast majority of modern scams are some form of phishing, and many data breaches (including the 2017 Equifax incident) are the result of an attacker obtaining login credentials from an insider through some method of social engineering.

---

[126] https://portswigger.net/daily-swig/mfa-fatigue-attacks-users-tricked-into-allowing-device-access-due-to-overload-of-push-notifications

Some examples of phishing:

- An email that demands payment (or notifies you of an automatic charge to your credit card) for goods or services you never ordered, and provides a phone number or email address for refunds and customer service requests.

- An SMS text message that says there has been fraudulent activity on your credit card or bank account, and asks you to respond with personal information (such as your Social Security number, account PIN or password, or 2FA code), or to call a phone number that isn't connected to your bank.[127]

- A letter in the mail that claims you won a contest or random drawing, but you have to call a phone number and "verify your identity" in order to claim your prize.

- A job posting that offers to pay an unreasonably high amount of money for doing an unreasonably low amount of work, requires minimal qualifications from applicants, and requests an unusual amount of personal information when applying.

- "Get rich quick" schemes that require personal information in addition to an upfront payment.

- An automated phone call (also referred to as a **robo call**) claiming that you owe money to the IRS, or that you've been fined for refusing to report for jury duty.

- A text message sent to your work phone from an unknown number in which the sender addresses you by name and claims to be your boss (who is also correctly named), and tells you that there's an emergency and you need to reply with the company credit card details immediately.

Remember my advice from Chapter 1: distrust by default all requests for payment? That's a good rule to define upfront because it's easy to remember and follow, but at this point you're far enough along on your *Privacy Crisis* journey that I'm comfortable asking you to broaden it: distrust

[127] *https://www.latimes.com/business/story/2021-05-25/chase-bank-fraud-alert-scam*

by default any request for personal information unless you initiated contact through official channels. If you get a phone call from someone claiming to be a representative of your bank, hang up immediately, then call the phone number that you are 100% sure is the correct one for your bank, and ask if there are any problems with your account. Perhaps it actually was a legitimate representative from your bank who called you, but when their first question is to ask you to provide your Social Security or bank account number to verify your identity, you should always assume it's a phishing attempt. Legitimate bank representatives are not ignorant of information security practices; if you challenge them, they will encourage you to call the bank on your own, but be careful – don't let them tell you which number to call! Call the number on the back of your debit card or the number published on your bank's website (just make sure it's actually your bank's real website first; as I'll explain later in this chapter, scammers often create fake websites that look just like the real ones, but the domain name is slightly different).

The last item in the list – the text message claiming to be your boss – is an example of **spear phishing**, which is a phishing attack that is highly personalized for the recipient. Most phishing attempts, by contrast, are broadcast to as many people as possible and aren't explicitly targeted at one person. Spear phishing is incredibly easy to do; while a thief could get a sufficient amount of personal information from stolen data on the Dark Web, it's quicker and easier to simply use publicly-viewable personal information on your social media accounts and in Web search results. Because of the amount of effort involved, spear phishing targets are almost always mid-level corporate employees (or any employee that has access to a company credit card or spending account) and high-value targets (as defined earlier in this chapter).

"Social engineering" generally refers to situations where someone tries to gain access to a restricted system, area, or account through deception. For instance:

- A thief affixes a printed memo to your company's office doors saying that there is a new (fraudulent) number to call for technical support.

- A scammer calls your bank and pretends to be you, and mumbles the responses to your security questions with the hope that the representative will continue without hearing the proper responses

either because of embarrassment that he or she doesn't understand the caller, or out of frustration from repeated attempts to communicate.

- A hacker claiming to be a Microsoft or Apple employee calls, texts, or emails to notify you that there is a critical unpublished **zero day vulnerability** (a security flaw in an app, device, or service that has not yet been patched) in the software running on every machine at your company, and he or she needs to know the Administrator password in order to patch it.

- A thief dressed as a delivery driver or courier enters your company's lobby seeking unrestricted access to the rest of the building, insisting that only the CEO (or some other executive or manager) can sign for an extremely important and time-sensitive document or package, and that anyone who causes delays will be fired.

- An unemployed medical student with a bag of golf clubs walks confidently into the office of a golf course, announces that he's "the pro from Dover," and asks, as a professional courtesy, to take the next available tee time free of charge.

SIM-Jacking

SIM swapping is the process of conveying a mobile service account from one device to another by transferring a physical SIM or by moving the account to a new SIM. This is not inherently bad or illegal; you do it every time you replace your smartphone with a new one. Without SIM swapping, you'd have to get a new phone number every time you upgraded to a new phone.

SIM-jacking is when a thief switches your mobile service account to a phone that he or she controls.[128] The thief can then intercept your 2FA codes sent via SMS text message (which is why I recommend using other 2FA methods when possible), and take control of your online accounts. Locking your SIM card with your mobile carrier (as I urged you to do in Chapter 1) prevents SIM-jacking to a certain extent, but if a thief has

[128] *https://us.norton.com/blog/mobile/sim-swap-fraud*

enough personal information about you, he or she can call your mobile service provider pretending to be you (social engineering) and answer the security questions required to unlock your SIM. If you provided unique dummy answers to your security questions, though, you should be perfectly safe.

Another method of SIM-jacking is to remove the SIM card from your phone (probably by stealing the phone, but possibly by just removing the SIM card without your knowledge) and install it in the thief's phone. Again, locking your SIM prevents moving it (unless the thief knows or can guess the unlock code). This method of SIM-jacking is slowly becoming obsolete. Older devices use removable SIM cards – a fingernail-sized microchip with a small amount of storage – which have to be physically removed from one device and installed in another; newer devices have non-removable eSIM or iSIM modules embedded into the phone's hardware.

Aside from SIM-jacking, there are other security concerns with removable SIM cards – particularly older ones. There have been multiple security vulnerabilities in previous generations of SIM cards that enabled three-letter agencies to monitor voice and data communications, and hackers to track the location of mobile devices.[129] If you're using a SIM card older than 5 years or so, I encourage you to get a new one from your mobile service provider (if your phone supports it).

Sloppy Software Development Practices

Some data breaches aren't the result of a clever attack or intrusion; they're just plain-old unforced errors on the part of the IT workers who develop and maintain an app or program.

In order to connect an app, website, or program to a service or data source, it has to have secret credentials just like humans do. Sometimes these secrets are in the form of a username and password, but more commonly it's an **API token** (a unique string of characters that identifies a particular developer or company who has permission to access a third-party service, similar in concept to a Social Security number) or a **cryptographic key** (a very long string of characters that enables a person or program to encrypt

[129] *https://en.wikipedia.org/wiki/SIM_card#Security*

and decrypt data). Sloppy programmers will print those secrets in the program's source code, hoping that various obfuscation techniques will hide them. That doesn't usually work, though; skilled hackers can still use a variety of methods to extract them.[130]

Typically source code is not published anywhere, and only the owner or a group of software developers has access to it. Often, though, software (in part or in whole) is **open source**, meaning its source code is publicly viewable so that a wider group of engineers can audit, modify, and contribute to it. Every change made to the source code must be documented so that its authorship and copyright can be validated, and so that a single change can be removed if it causes problems later. The standard method of managing source code in this way – whether it is open source or not – is through a management framework called a **source code repository**.

When a developer doesn't remove a program's secrets from the source code before committing it to a public repository, he or she has published them for all to see. That's like tweeting your X / Twitter username and password. This kind of mistake happens frequently, and it isn't always properly remediated when it's reported to the project's maintainers. Since the repository keeps a full history of all code changes, a developer cannot simply erase the secrets and commit the revised source code (though that's a good first step). Even if the history can be erased, someone may have downloaded it already. The only viable solution is to create new credentials and invalidate the old ones, and ensure that the new secrets will not be committed again. Unfortunately a lot of developers and project maintainers don't take these steps after they've leaked their secrets.

Another type of data breach related to software development is when engineers or quality assurance testers use private data (from customers, employees, or users) for testing, evaluation, or demonstration purposes. When software is being actively developed it often does not have any of the safeguards (such as encryption and authentication) in place that would be added when it's ready to ship or publish. That potentially exposes any data it handles. Even if this data leak is only internal to the company that is developing it, private data can be viewable to employees who do not have permission to access it. The right thing to do is to generate dummy

---

130 https://www.forbes.com/sites/forbestechcouncil/2024/04/30/the-danger-of-zombie-leaks/?sh=312950b8273d

data, or use data from a public source, but sometimes programmers are lazy and take shortcuts.

Unpatched Software

As consumers we're constantly hassled to update the software on our computers and mobile devices, sometimes to fix bugs that cause usability or stability problems, but more importantly to address security vulnerabilities that could enable hackers to remotely break into our devices. Fortunately these updates are usually easy to apply through automated frameworks like Windows Update and the Google Play Store. Click or tap a few buttons, and updates are applied, usually on a weekly or monthly basis. Unfortunately, small companies and individual software developers who can't afford to (or don't want to) buy into the update frameworks of big tech companies have limited options for notifying their users of security issues, and providing patches or new versions to address them. So if you download and install an app or program outside of those frameworks, then you probably won't be notified when there's a new version or a critical security patch to apply. Consequently you could be running an outdated program or app that has a widely-known security flaw; it's up to you to check for security updates for anything you install outside of your operating system's official software store or package manager.

When you run a server (to provide email, websites, media streaming, or other connected services), updates are not always automatic because the changes they make can be disruptive, so it's up to the system administrator or IT manager responsible for that server to decide which updates to apply, and when to apply them. Good system administrators stay current with all of the latest security updates and apply patches quickly, but there are a surprising number of IT professionals who are lazy or incompetent; they barely managed to get the server working a long time ago (or it was originally set up by someone who is no longer at the company), and are afraid to apply any updates that might make configuration changes or cause other issues that disrupt the services they're paid to maintain.

Even when a company has reasonably competent IT staff, security vulnerabilities can still go unpatched when the company's IT infrastructure includes one or more low-level services that "just work" and have been running silently behind the scenes for such a long time that no current employees know how to maintain them. In some cases those systems may

be so highly customized and undocumented that no one knows how they work, or that they even exist.

Lastly, sometimes there are rogue programs that were installed without permission. IT managers typically lock-down a company's computing environment so that no unauthorized software can be installed on any company-owned device. However, when an employee needs to install an unapproved program or browser plug-in in order to get his or her work done, the delays and denials of corporate bureaucracy may drive them to secretly install the software they need. If they can't install it on their company computer, then they might bring their own personal computer to the office (or use it when working from home) – which could contain any number of unpatched programs or even malware that can lead to a corporate data breach.[131]

Unpatched Firmware and Backdoors

Similar to unpatched software running on mobile devices and PCs, individual hardware components and IT appliances can have remote security vulnerabilities.

One of the most common examples of this is network routers, which are easily ignored as an IT appliance that "just works" and doesn't seem to need active maintenance. Like many IT appliances (printers, peripherals, add-on cards, etc.), routers – especially wireless routers, including the one you use in your home – run on a kind of immutable software known as **firmware**. While firmware cannot usually be altered directly, it can be wholesale replaced with a firmware update, which you must manually initiate – it is never automatic (unless the firmware is controlled by the operating system, which includes the internal components of most computers and mobile devices). Updating firmware is usually a relatively quick and easy process through the router's Web interface or corresponding desktop or mobile app. Again, though: if you don't manually update the firmware, it won't be done for you. If there are no security holes in your router's firmware then there's usually no reason to update it, but the factory-default firmware installed on many routers often contains one or more vulnerabilities that were discovered after the device was shipped. Hackers actively search for networks that use routers and

[131] *https://proton.me/blog/lessons-from-lastpass*

modems with unpatched firmware. In many cases they're able to break into routers that have security holes that are several years old; the owners never bothered to update them.

When security holes are intentional instead of accidental, they're referred to as **backdoors** because they allow someone to sneak into a device or network through a secret entrance that circumvents normal authentication and/or authorization controls. There are a few different paradigms for backdoors:

- A hacker is able to break into a device with elevated privileges (the root, superuser, or administrator account), usually through phishing or brute force, then secretly installs a program (known as a **rootkit**) that will enable them to continue to gain elevated access in the future without detection.

- A user downloads and runs a trojan horse (this is explained in detail in the next subsection), which installs a backdoor service.

- A hacker or three-letter agency intercepts a device or device component during transport (from a component supplier to a device manufacturer, or from a warehouse to a store, or from a store to a customer), and overwrites the default firmware with an otherwise identical version that includes a backdoor.

- Software – in the form of an operating system, server program, device driver, or firmware – includes a secret function that will allow remote access or low-level control by the device owner, manufacturer, or a three-letter agency.

- Similarly, an undocumented piece of hardware or a hidden register within an integrated circuit allows remote access and control; this is at a lower level than the operating system, so it can be very difficult to detect and potentially impossible to close with a patch or firmware update.

Backdoors implemented by the software developer or hardware manufacturer are usually not intended to be used for nefarious purposes. Often they were created to assist in development, debugging, and testing, and were not removed or disabled afterward. Some backdoors are included by design; for instance most mobile devices have backdoors (which are accessed by turning the device off, then holding down or pressing a

sequence of buttons while it powers up) that enable someone to remove a carrier-specific lock or overwrite the manufacturer-provided operating system with an alternative. This doesn't grant access to encrypted data, but it does enable low-level potentially destructive capabilities that don't require authentication.

International cyberwarfare and espionage are a substantial factor in backdoor installation and exploitation via a **supply-chain attack**, which is when hackers focus on the third-party components, devices, or services used by their ultimate target. For instance Russian state-sponsored hacking groups have been caught exploiting remote vulnerabilities in consumer-grade printers and routers to install rootkits that are then used to install malware, the ultimate purposes being to create a **botnet** (a widespread collection of compromised network-connected devices that can be remotely commanded to execute a coordinated **DDoS**, or **Distributed Denial-of-Service**, attack), to steal secret information, or to execute a ransomware attack.[132] The hacking group known as "Anonymous" has also used backdoors in Russian printers to print multiple copies of documents containing Russian-language instructions for downloading Web browsers that can bypass state media censorship measures, and a message that Vladimir Putin is lying about the details of his invasion of Ukraine.[133] Even as far back as 1982, the CIA was tech-savvy enough to intercept a shipment of software bound for the USSR and secretly alter it in a way that caused an explosion in a Siberian gas pipeline; today they would almost certainly opt to install a backdoor instead, which would enable them to remotely gather intelligence and dictate the exact time and conditions for sabotaging the pipeline controls.[134]

It's impossible to know for sure whether there are backdoors built into any of the millions of highly complex IT hardware devices currently in service. The manufacturers themselves may not even know because their products are composed of hundreds of components sourced from various third-parties, and as a rule any kind of backdoor would be undocumented, and if it were mandated by a three-letter agency then it would be illegal to

---

[132] https://www.techradar.com/pro/security/microsoft-says-russian-hackers-are-exploiting-an-ancient-printer-security-flaw

[133] https://www.newsweek.com/anonymous-hacks-russian-printers-deliver-resistance-information-1690269

[134] https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/

disclose it. There have been a few notable instances where hardware manufacturers have been caught red-handed, though:

- Several generations of Intel chipsets and processors are known to contain backdoors (many of which cannot be closed through driver or firmware updates without vastly reducing the processor's capabilities), though they are largely believed to be legitimate engineering flaws.[135][136] However, I do know that Intel intentionally included an undocumented register – at the behest of the NSA via its High Assurance Platform (HAP) requirements – that disables its also-undocumented Intel Management Engine (ME) chip.[137] ME enables remote low-level access to Intel-based computers; it grants secret access to memory and network communication even when the computer is powered off (ME can power-up the device), and cannot be definitively disabled other than through the (formerly) secret HAP bit. This is, by definition, a backdoor; Intel claims that it is strictly designed for companies to remotely manage all of their computers.[138][139]

- According to reporting by *Bloomberg,* as far back as 2010 and possibly continuing to the present day, PC and server motherboards manufactured by Super Micro Computer (aka Supermicro) contain secret, undocumented chips that provide backdoor access to Chinese military intelligence.[140] Supermicro motherboards are used in a wide variety of servers at nearly every major IT service-provider in the US. Supermicro – and companies that use servers containing Supermicro motherboards such as Amazon and Apple – deny these

---

135 https://www.techspot.com/news/100814-intel-knew-about-downfall-cpu-vulnerability-but-did.html

136 https://hackaday.com/2020/06/16/disable-intels-backdoor-on-modern-hardware/

137 https://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html

138 https://www.csoonline.com/article/562761/researchers-say-now-you-too-can-disable-intel-me-backdoor-thanks-to-the-nsa.html

139 https://www.techrepublic.com/article/is-the-intel-management-engine-a-backdoor/

140 https://web.archive.org/web/20240206223748/https://www.bloomberg.com/features/2021-supermicro/

claims.[141] On the other hand, they would be required by law to do so if asked.

Trojan Horses (Illegal)

Earlier in this chapter I defined "trojan horse" as any software, device, process, service, or activity that pretends to be helpful or benign, but secretly serves a harmful purpose, and I described some ways that marketers legally (usually) trick people into giving away personal information. Scammers can also use those tactics for nefarious purposes, even if the methods they use to collect information are technically legal. It is not illegal, after all, to ask someone for their Social Security number or bank account details; it is not even illegal (as far as I know) to trick people into revealing that information. It is, however, illegal to use it to steal from them or commit fraud in their name.

In the more traditional technological sense, a **trojan horse** is a program or app that a hacker tricks someone into installing on their computer or mobile device. It pretends to do something amusing or useful, but its true purpose is to enable the hacker to steal information or remotely use the device for some other nefarious purpose. The secret "payload" of a trojan horse is usually one or more of the following:

- **Keylogger:** records everything you type (or only records what you type into account credential fields) and sends it to the attacker.
- **Backdoor:** provides remote access to a device and all of the information on it, sometimes including data you've encrypted.
- **Bitcoin miner:** a process that runs in the background, mining Bitcoin for the attacker. This is not usually harmful for the victim, but it does consume a lot of system resources and therefore electricity and network bandwidth, and reduces system performance.

[141] *https://9to5mac.com/2021/02/12/super-micro-spy-chip-story/*

- **Ransomware:** encrypts your hard drive and demands a ransom payment (typically in cryptocurrency such as Bitcoin or Monero) in exchange for the encryption key.

- **Zombie DDoS node:** a lightweight process that listens for a remote command to use your device (along with many others that have also been compromised) to bombard a server with many useless requests (a DDoS attack). To be effective, the attacker must successfully acquire a multitude of zombie nodes to create a botnet.

Occasionally hackers and foreign agents can successfully develop a legitimate-looking trojan horse app (such as an alternative SMS messaging or social media client, or mobile game) and get it into a legitimate mobile app store for a while before they're caught and removed. More commonly, though, the trojan horse is something that a person downloads outside of a sanctioned store or software framework; they **sideload** a mobile app by downloading it from a website and circumventing the app management framework to install it directly, or download a program from somewhere and install it on their computer. While any kind of software can potentially be (or contain) a trojan horse, these are the most common vectors:

- **Software activation cracks and license key generators.** These are programs that generate license keys and/or bypass software activation features of commercial software, allowing people to use commercial software for free. This is less common today than in previous eras when popular proprietary software like Microsoft Office and Adobe Photoshop had expensive license fees and yearly upgrades (both are now delivered as much more affordable software-as-a-service schemes).

- **Cracked or "pirated" software.** This is expensive commercial software that has already been hacked to bypass the license key and activation functions. Again: this is not as common as it used to be.

- **Game cheats and boosting services.** Similar to software activation cracks, these programs alter game software and network traffic to enable people to cheat in online games (such as aimbots, wall hacks / ESP, and map hacks). To avoid getting

caught cheating, some people will pay for "boosting" services, where they give their account credentials to someone else (ostensibly a very skilled player, but more likely someone who is using game cheats) who will play the game for them and raise their player level, skill ranking, or competitive rating. Once the "boosters" have control of the game account, they can then sell off any in-game assets, or sell the entire account; and even if they don't scam their customers, the account can still be flagged for cheating and banned from the service.

- **Pornography.** This is one of the oldest trojan horse delivery vectors, though its methods have evolved over the past three decades.[142] Generally you are safe viewing (legal!) pornographic images and videos online; the trojan horses are largely in downloadable archives of photos or videos either from the Web or in email attachments, and in the ads on porn sites. Never click on or download anything pornographic from an email (or, really, anything at all from any unknown sender, or from a known sender whose email account may have been hacked), and never click on external links or ads on any porn site you visit. Even if the porn site is legitimate, the owners don't always properly vet their advertisers, and hackers have hijacked ad banners on porn sites in the past.[143] There have also been cases where illegal pornography was copied onto people's computers via a trojan horse, and the attackers reported them to authorities.[144] Porn-based trojan horses are so pervasive that the mere threat of them is a scam in itself: there is a common blackmail scheme where the attacker sends an email claiming to have evidence of the victim's porn consumption (a screen shot, stolen login credentials, or a secret webcam video), and threatens to post it on the Internet or send it to his or her email contacts unless a ransom is paid.

- **Microsoft Word or Excel documents.** Microsoft Office documents can contain scripts that install malware. Modern

[142] *https://www.wired.com/1997/06/dont-touch-that-porn-trojan-horses-hit-aol/*
[143] *https://www.komando.com/security/porn-site-malware/757172/*
[144] *https://www.zdnet.com/article/trojan-horse-found-responsible-for-child-porn/*

versions of MS Office are configured to prevent scripts from running when you open downloaded files, but users can simply click a button to override this safety feature. Regardless of the file type, don't download any email attachment that you aren't 100% sure is both necessary and legitimate, even if it's from someone you know – their email account may have been compromised and used to send out trojan horses, spam, or phishing schemes.

With the exception of MS Office documents, secrecy and shame are the common themes among trojan horse delivery vectors; the people who download these programs don't want anyone to know about it. This in itself presents an excellent extortion opportunity for thieves who create trojan horses and can identify their victims. The first two items in this list are plainly illegal; they violate copyright and software piracy laws. Game cheats are not generally illegal to use, but using them violates the terms of service of every modern online game, which will result in the cheater's account being (usually permanently) terminated without refund, along with every in-game purchase they've made – and people who are vain enough to cheat in competitive video games are inherently fearful of being outed as cheaters. In some parts of the world, pornography is illegal to possess in any form; even in the Western world some kinds of pornography are illegal, and generally consumers of legal pornography prefer to keep their porn habits and preferences a secret.

Third-Party Service Intrusion

As I illustrated in the Blackbaud case study earlier in this chapter, when a company entrusts critical business services – especially those that handle personal data for employees and customers – to a third-party vendor, it can no longer guarantee that the information is safe. Unfortunately it's nearly impossible for modern businesses to avoid using third-party services to handle employee and customer data. The best a manager or business owner can do is thoroughly vet each prospective vendor, disable all non-essential options and features, and never entrust them with anything more than the bare minimum information.

Sometimes the data handled or stored by a business-to-business (**B2B**) service provider is the prize (such as with Blackbaud), and sometimes it is only the means for executing a larger data breach at one or more of that

company's client organizations – a different kind of supply-chain attack than the hardware-based examples I used in the "Unpatched Firmware and Backdoors" section earlier in this chapter. Hacking into third-party services is often the easiest method of intrusion into highly secure companies and government offices by foreign intelligence groups and three-letter agencies. For instance if hackers working for the Chinese, North Korean, or Russian government cannot break into a US Department of Defense database directly, then they will try to find out which commercial third-party services the DoD uses, and hack into them instead.

In fact that exact scenario happened in late 2020 when a sophisticated hacking group believed to be associated with the Russian government infiltrated SolarWinds, a US-based company that provides a suite of IT management tools.[145] The attackers were able to gain access to SolarWinds' internal company network, then install a backdoor in the source code of its Orion network management platform. It was then delivered to SolarWinds' clients through a scheduled software update. The backdoor enabled the attackers to log into any of SolarWinds' customer systems with any of their user accounts without detection. Since the Orion platform has access to IT secrets, the hackers were then able to break into those customer networks via the Orion backdoor. More than 18,000 SolarWinds customers were vulnerable to remote intrusion, including Microsoft, Intel, FireEye, and the US Departments of State, Homeland Security, Commerce, and Treasury.[146]

Evil Service Technicians

When you bring your computer, tablet, or smartphone into a repair shop for service, you're often giving the technicians – and anyone else who works there – total access to everything stored on those devices. If the data is encrypted, then you're reasonably safe because they cannot access anything without your password / PIN / fingerprint, or other method of

145 https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
146 https://www.npr.org/2020/12/21/948843356/how-a-cybersecurity-firm-uncovered-the-massive-computer-hack

authentication. (They could still SIM-jack you if your SIM is unlocked, though).

However, repair technicians often say that they need you to unlock your phone or log into your computer's administrator account so that they can run diagnostics or validate the repair they've made. This isn't always true. Even when it is, I recommend you don't do it unless you feel it's absolutely necessary and you are able to closely supervise what the technician does while the device is unlocked.

Desktop and laptop computers can boot from USB drives or optical discs for diagnostic purposes, or can be accessed on a minimal basis via a "guest" account without granting access to any stored data in your main user account. Mobile devices – smartphones, smart watches, tablets – don't usually have these options. Granting unrestricted and unsupervised access to your smartphone could be disastrous; a stranger will be able to use any of your apps that don't require authentication (beyond unlocking the phone), view your mobile browser history, and view and copy any files stored on the device, even if they're encrypted (they are decrypted when the device is unlocked).

Most service technicians are smart enough to know that they won't get away with using your mobile apps for nefarious purposes. However, several have been caught viewing and even copying nude photos from customers' smartphones.[147][148][149][150]

I'm not going to tell you not to take nude photos of yourself or even pornographic videos (assuming you have the explicit permission of anyone else involved), but I urge you not to send any of them to others via electronic means (MMS text messages, email, social media, etc.), and to store them only on zero-knowledge end-to-end encrypted storage services

---

[147] *https://www.tomsguide.com/news/iphone-repair-technicians-violated-womans-privacy-by-posting-her-photos-online-apple-reportedly-paid-out-millions*

[148] *https://www.androidpolice.com/google-pixels-warranty-stolen-nudes-hijack-accounts/*

[149] https://www.msn.com/en-us/money/technology/repair-techs-at-best-buy-mobile-klinik-and-more-caught-looking-at-customer-data-nudes/ar-AA1iAxD8

[150] *https://nypost.com/2022/05/19/the-modern-day-peeping-tom-how-creeps-steal-nudes-off-phones/*

(such as Proton Drive) or on removable media that you can lock securely in a safe. Never store nude photos or videos on your phone.

Mail Theft, Dumpster-Diving, and Secondhand Computers

The oldest method of obtaining personal information for identity theft purposes is intercepting the victim's mail, either directly from their mailbox or by digging through their trash to look for discarded bank statements and other documents. This applies even moreso to the dumpsters and recycling bins at office buildings and corporate campuses.

In the modern era this is a little less useful to residential thieves than it used to be because many people have gone "paperless" and no longer receive potentially valuable mail, and financial institutions no longer print full account numbers on mailed statements, but it's still a huge risk for identity fraud. Incredibly, printed utility, cable, cellular service, or other bills (and signed lease agreements) – all of which are easily counterfeited – are still used as legally-required "proof of address" in many instances, such as:

- Reserving a PO box
- Initiating a change-of-address with the Post Office
- Establishing a new home-based service such as cable TV, Internet, or filtered water delivery
- Obtaining local resident benefits (such as Florida resident annual passes at Walt Disney World, or access to a community center)
- Obtaining or changing the address on a government-issued ID
- Opening a bank account
- Establishing insurance coverage for a home or vehicle
- Obtaining credit, especially to purchase a used car

Additionally a utility bill is often all a squatter needs in order to legally establish residency in a home, even if he or she doesn't have a deed or lease. This includes roommates and temporary guests. In many jurisdictions, if you allow someone to stay in your home for any length of

time and they receive a mailed bill or statement in their name at that address, then they can use that document as proof that they have a legal right to live there. To legally remove them, you'll have to go to court and file an eviction.

Shredding all documents before you discard them is generally a safe method of deterring dumpster-divers. For maximum protection (or if you're shredding documents for a business), use a cross-shredder, or mix up the pile of shredded documents and throw them away one clump at a time over a period of weeks so that they cannot be reassembled from a single dumpster-drive incident. When disposing of credit cards, you should shred them (but only if your shredder has a dedicated credit card slot), or cut them into many pieces with scissors and put them into different trash cans.

It's important that you retrieve your mail as soon as you can. If you will be away from home for a while and no one will be there to receive it, ask the Post Office to hold your mail until after you return; it will be collected while you're gone, then delivered on the date you specify. Also, if you happen to receive mail addressed to someone else, do not open or discard it; you must write "NOT HERE" or "NOT AT THIS ADDRESS" on the front of the envelope, and put it back in the mailbox with the flag up shortly before your mail carrier usually arrives (not overnight, if possible). This officially notifies the sender that the addressee does not live there, which prevents identity thieves from establishing themselves at your residence.

Lastly, thieves often find personal data on used computers that are either thrown in the trash, or sold on Craigslist, eBay, or Facebook. Before discarding or selling any of your old computers, tablets, e-readers, or smartphones, ensure that the permanent storage has been completely wiped and reformatted back to the factory default operating system, and that there is no removable media in them (such as CDs, tapes, optical disks, SD cards, or SIM cards). Businesses disposing of retired PCs should go one step further and either physically destroy the hard drives (which is what three-letter agencies do), or use a utility to perform a low-level or "zero fill" format to ensure that deleted files cannot be recovered via conventional forensic tools.

The Disgruntled Employee

The vast majority of data breaches are the result of brute force attacks, phishing, or exploiting an unpatched vulnerability in a company's servers, but approximately 5% of cyberattacks (which include data breaches, ransomware, and internal email intrusion) are "inside jobs" committed by disgruntled current or former employees.[151] For some people the motive is probably revenge, but others may seek profit in selling stolen data on the Dark Web or elsewhere. If you're in charge of any kind of organization, treating your employees and contractors with dignity and professional courtesy – especially when they're fired or laid-off – can remove the motivation for committing these kinds of data breaches.

Just as importantly, try to avoid patronizing businesses that treat their employees badly. Consider for a moment how easy it would be for an HR assistant, office worker, secretary, or clerk to steal or copy your secret information for selfish purposes.

Domain Hijacking

You should always ensure that a URL matches the website you're intending to view. For instance the official site for Capital One Bank is `www.capitalone.com`. Spammers and scammers like to try to reserve domain names that are similar to official sites, with the hope that they'll fool visitors into thinking that they're at the correct URL. This often involves using homonyms, dashes, and typos. For instance these could look like the Capital One site, but in fact are not (don't go to any of these URLs – this is strictly for example purposes):

- capital-one.com
- capital1.com
- captialone.com
- cappitalone.com

[151] *https://www.informationweek.com/cyber-resilience/75-of-insider-cyber-attacks-are-the-work-of-disgruntled-ex-employees-report*

- capitalone.ru
- capitalone-official.com

Personal information – especially secrets – are often stolen by creating lookalike sites (sometimes they're even an exact copy of the official site) hosted at URLs that are similar, but not exact. At a glance (or if you're a terrible speller), it looks legitimate. Scammers will even buy ads on Facebook and other online platforms claiming to be a bank or online retailer, but when you click on them you go to a lookalike scam site. Because of the opportunity for fraud, smart businesses buy up as many of those close-but-not-exact domain names as they can, and either leave them blank or redirect them to the correct URL.

Sometimes even an official domain name can be hijacked, though, via two methods:

1. **Unauthorized transfer**: an attacker can request a transfer of a domain name from the victim's registrar to theirs. You can prevent unauthorized transfers by locking your domain. This is a free feature offered by all commercial domain registrars, but you usually have to manually opt-in to it.
2. **Infiltrating the victim's registrar account**: by using one or more of the intrusion methods defined earlier in this chapter, an attacker can learn or guess the victim's login information for their domain registrar and take over their domain names. You can prevent thieves from breaking into your domain registrar account by taking the information security precautions I've covered in detail in Chapters 1 and 2.

When a hacker gains control of an official domain name, he or she can harvest login information, intercept email, and steal any data that the site owner would have access to.

Lastly, sometimes domains expire because the owners fail to renew their domain registration. If a person dies or a business closes, there may simply be no one who has the authority or interest in renewing it; however, it also happens by accident quite often. Even huge corporations like Microsoft,

Regions Bank, and the Dallas Cowboys NFL team have failed to renew domain names that were critical to their operations.[152][153][154]

Once an established domain name expires, spammers and scammers immediately rush to take it over. This isn't illegal; you're allowed to buy expired domain names. When it happens by accident, though, the new domain owner can use it for spam or scam purposes, or to extort the previous owner in various ways.

Expired domains don't immediately go up for auction. Domain registrars are required by ICANN to provide customers with at least three renewal notices prior to their domain expiration, and must allow a 30-day redemption grace period after the expiration date to account for extraordinary circumstances.[155] Those are the mandated minimums; registrars are free to send more notices and provide longer grace periods.

Malicious Data Injection and Cross-Site Scripting (XSS)

Another way hackers can steal personal data and secret information from visitors to legitimate websites is by tricking the site into thinking it's loading and serving its own code (usually in the form of Java, JavaScript, ActiveX, or VBScript, but possibly also HTML) when it is actually using something malicious. Essentially this is a method of phishing that targets software instead of people. There are a variety of ways to accomplish this, but they're highly technical and I don't want to burden you with the details; suffice it to say: it's the result of shoddy Web development practices. A properly designed and developed website or Web application is rarely vulnerable to these kinds of attacks.

152

https://web.archive.org/web/20140627124327/http://www.webip.com.au/major-bank-forgets-to-renew-domain-name-entire-online-operation-goes-down/

153 https://www.cnet.com/news/cowboys-fire-coach-forget-to-renew-web-domain/

154

https://web.archive.org/web/20081012193400/https://slashdot.org/articles/99/12/25/114201_F.shtml

155 https://www.icann.org/resources/pages/domain-name-renewal-expiration-faqs-2018-12-07-en

Chapter 4: The Direct Consequences of Surrendering Your Data

Thus far I've mentioned a few things that can go badly for you if your personal data falls into the wrong hands, with an emphasis on criminal activity. But stealing from you isn't the only way for others to enrich themselves at your expense. It isn't enough to protect things that are worth stealing; you must also protect yourself from being influenced or coerced into making decisions that benefit others at the expense of your time, money, health, and safety. In this chapter, I'll go into more detail on the various ways that your personal data can be used against you to enrich selfish people and greedy corporations.

Con-artists and psychopaths have always been able to exploit our evolutionary gifts to service their evil plans. They are charming and charismatic, which makes it easy for them to seem sincere when they share false information, and to trick honest people into revealing critical details about themselves. When one of these predators has enough information about you, he or she can begin to manipulate you into being an accomplice in – and later, a victim of – their schemes. Fortunately these broken people

rarely prosper for very long, and aren't typically very good at evading punishment for their actions.

More recently the Internet enabled much larger entities – corporations and governments – to take advantage of our innate need to share, for the marginally less evil purposes of targeting us with advertisements, political propaganda, and disinformation. The more an advertiser knows about you, the better enabled it is to show you an ad you'll click on, or a false message that is likely to change your opinions or beliefs.

As social animals, it is extremely difficult for human beings to resist the urge to share information about themselves in social settings. Sharing our stories is how we connect to each other; it's how we form friendships, romantic relationships, and business partnerships; it enables us to create communities so that we can pool our resources to achieve collective goals. If you don't share your stories with people, then you cannot connect to them, and you'll lose out on the irreplaceable benefits of human society. We've evolved to behave this way because historically it has benefitted us as a species, so I'm not going to tell you never to share with other people – that would be ridiculous – but you must be conscious of *what* you share and *whom* you are sharing it with, and be mindful of who else could potentially be eavesdropping or recording the conversation.

Unless you're a spy or a criminal, you don't usually have to be too cautious about casual conversations in public places like restaurants or sports games, though you still don't want to reveal anything that would make a victim out of you if a professional thief were to overhear it, such as: "I left my purse in the car," or "I still have those $100 bills in my wallet." Be *very* cautious of what you share online, though, because it's at best difficult – and at worst, realistically impossible – to remove information from the Internet after it's been published.

In this chapter I'll explain the most common and likely ways that you will be negatively impacted by losing control over your personal data.

Virtual or Electronic Harm

Crime and commerce are indelibly connected; wherever commerce goes, crime – in its many forms – follows. Therefore in a world that is increasingly digital, the modern thief's toolkit is more likely to include a credit card skimmer than a lockpick. As strange as it may seem, though,

having your credit card skimmed and used to make unauthorized charges is perhaps the least harmful thing a digital thief can meaningfully do to you. Fraudulent credit card charges can easily be challenged and reversed, but it's much harder to repair the damage from scams and identity theft. The most common and popular ways to use people's private data to scam, exploit, or steal from them are detailed in the subsections below.

Identity Fraud

Identity fraud is the act of using another person's personal or private information to engage in any unauthorized financial commitment or legal obligation under their name.[156] For instance:

- Creating a financial account (checking, savings, investment, retirement) or applying for a line of credit
- Signing or co-signing a lease, loan, or contract
- Obtaining health care services or prescription drugs
- Shirking legal responsibility for civil or criminal law infractions
- Qualifying for unearned government benefits or other resources intended for someone else (tax refunds, social security payments, unemployment compensation, economic stimulus funds, Medicare or Medicaid benefits, military benefits, food stamps)
- Filing false insurance claims
- Applying for a job
- Selling real estate
- Voting in an election
- Taking control of mobile devices, digital assets, and service accounts

Identity fraud begins with **identity theft,** which involves obtaining sufficient personal information to enable a thief to create documents that

[156] *https://www.usnews.com/360-reviews/privacy/types-of-identity-theft*

falsely identify the perpetrator as the victim.[157] For instance an identity thief could fabricate a state-issued driver's license containing your name, address, date of birth, and ID number, but instead of your photo and physical description, it's the thief's. By using some of your legitimate personal information to create falsified credentials, the thief will then go on to borrow money, obtain credit, and shirk his legal responsibilities onto you. If his false driver's license is good enough, it can even fool the police; you could be arrested for failing to appear for a civil or criminal court date pertaining to a crime or infraction that you didn't commit.

By far the most common forms of identity fraud are not so extreme, though:

- Hijacking your social media accounts or websites to post spam, scams, or disinformation.
- Applying for a credit card, then using that card to purchase things that are difficult to trace and can be quickly resold, such as prepaid gift cards, online game subscription cards, and long-distance calling cards.
- Stealing tax refund, Social Security, and welfare money from rightful beneficiaries.

Credit bureaus and financial institutions assume that anyone who can provide a reasonable amount of your personal and private information is either you or someone who has lawful power of attorney to represent you. That is why it's so important to keep as much of your data off of the public Internet (and out of your trash can) as possible, and to only give the bare-minimum information to companies you interact with.

Actions you can take to make identity fraud more difficult, in addition to the ones I've already covered:

1. Remove your date of birth, middle name or initial, and home address from all websites that you control.
2. Opt-out of "pre-approved" credit card offers.

---

[157] https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

3. Opt-in to "paperless billing" for all of your utilities and financial accounts (unless you're using a PO box for all billing correspondence).

4. Pay close attention to your credit card activity. If your bank or credit card issuer has a feature that notifies you of new charges by email, text message, or app notification, turn it on.

> ➢ NOTE: If you suspect that you may presently be a victim of identity theft, contact all three consumer credit reporting agencies immediately, and request that a **fraud alert** be placed on your credit files. This will stop new fraudulent accounts from being created, and make it easier to remove existing ones. For further assistance, contact the non-profit Identity Theft Resource Center: `https://www.idtheftcenter.org`

Theft of Cash

Given a choice, thieves will almost always choose to steal cash above all other assets. It's easy to hide, mostly untraceable, and – with the exception of drugs or food – it's their ultimate goal anyway. There are four ways to steal cash in the digital realm:

- **Wiring money out of a bank account.** It's frighteningly easy to wire money out of an account, and unless it is obviously fraudulent (if you had absolutely nothing to do with it), you cannot get that money back. This is more of a concern for victims of scams who willingly initiate a wire transfer under false pretenses, but any skilled digital thief can drain your bank account if he has enough information about you and your bank.

- **Sending cash with an app.** There are several mobile apps that enable users to send cash quickly and easily to other people. Unfortunately "quick" and "easy" are antithetical to security and privacy. Again, this is more of a concern for victims of scams who willingly transfer money to scammers, but you should still take action to make it as difficult as possible for skilled digital thieves. While it's possible for thieves to steal or SIM-jack your mobile

phone to access your cash transfer apps, it's much easier for them to steal your identity and create a new account in your name.

- **Withdrawing cash from an ATM.** All someone needs is a card and a PIN, and your cash becomes theirs. Thieves install card skimmers on ATMs, gas pumps, and point-of-sale devices, then surveil the PIN keypad by standing nearby and "shoulder surfing" or by installing a hidden camera or keypad logger. According to the FBI, more than $1 billion is stolen each year by these methods.[158]

- **Purchasing goods or services with cheques, debit cards, or credit cards.** Fraudulent debit and credit card charges can be reversed simply by calling the card issuer and reporting them, but if your checking account is overdrawn by a large fraudulent debit card purchase or withdrawal, then you may have to fight with the bank to remove automatic penalties and fees. Fraudulent cheques are very easy to create, which is why handwritten cheques are rarely accepted as payment anymore, but they are still useful for setting up fraudulent direct debit payments for rent, loans, etc.

Actions you can take to make it more difficult to steal your cash, in addition to the ones I've already covered:

1. Narrow down your cash-transfer and "easy payment" apps and services to just the ones you really want, need, or regularly use, and uninstall all others from your mobile devices (including old phones that you don't use anymore). Limit yourself to one device only – uninstall cash-transfer apps from all but your primary mobile device.

2. Stop using personal checks, and destroy your paper checkbook if you have one. If you must send a check, arrange to have your bank print and mail a cashier's check to the payee. This service is usually free. If you need to present a check in-person, you can get a cashier's check from your local bank branch, or obtain one or more Money Orders (which can be traced and potentially revoked if stolen) instead.

---

158 https://www.capitalone.com/learn-grow/privacy-security/credit-card-skimmers/

3. Avoid using your debit card unless absolutely necessary. If possible, use it only as an ATM card.
4. Real-world cash theft is still a legitimate problem. Only use ATMs that are in safe, populated areas, and are maintained by financial organizations that you've heard of (preferably your bank). Don't use or even approach an ATM if there seems to be someone loitering nearby.
5. If your bank offers the ability to block all outgoing wire transfers, opt-in to it. Legitimate wire transfers are rare; you can disable the block later if you need to.

Account and Digital Asset Theft

A service account can be valuable to thieves for several reasons, depending on the type of account, as explained below.

Games

Online game accounts that contain rare items or high amounts of in-game currency can be worth hundreds or even thousands of dollars. The online game asset black market is big enough that it's become its own industry, including marketplaces for in-game items, game accounts, and in-game currency; cheat sellers; private game server hosting; and account boosting services.

At the slightly more legitimate (but still prohibited by game developers and gaming service providers) end of the spectrum, there are "gold farms" – offices full of people (usually in China) who are paid a small hourly wage to earn in-game currency, which is then sold to other players for real money.

Social Media

A social media account is primarily valuable to spammers and scammers who will take advantage of your legitimate account by posting links that your friends and followers are likely to inherently trust.

If you use a social media platform as a single sign-on solution for various other sites, services, and apps, then your social media account can be much

more valuable to thieves because it can enable them to make purchases as well as expand their spamming and scamming on a wider scale.

Cryptocurrency and Web3 Services

As of this writing, the fastest-growing and most profitable scams on the Internet involve stealing or intercepting people's cryptocurrency. Because it is impossible to reclaim and difficult to trace, digital asset theft is particularly important to state-sponsored hackers in embargoed nations such as North Korea, Russia, and Iran.

It's difficult to enumerate every way someone can potentially steal cryptocurrency because the scams in this industry are extremely clever and constantly evolving. As of this writing, the most common scams follow three basic paradigms:

1. **Sending an unsolicited non-fungible token (NFT) to an account.** When the NFT is claimed, the smart contract will deduct a fee from the recipient and send it to the sender.

2. **Investment scams,** where the victim is asked to transfer some cryptocurrency to someone else, with the expectation that an even larger sum will be sent back.

3. **Wallet scams,** where a scammer tricks victims into providing their 12- or 24-word recovery phrase.

Here are some ways to avoid crypto scams and keep your wallets secure:

1. Never accept an unsolicited NFT, especially if it promises a gift or reward. Sometimes genuine NFTs are sent from wallet providers, DeFi (decentralized finance) platforms, and staking services, but at the very least examine the smart contract first to see if there is a fee or any kind of transfer required of you. There is no fee to burn an unwanted NFT.

2. Never keep your wallet recovery phrases online (such as in cloud storage, note-taking apps, or email). The possible exception to this is a strong end-to-end encrypted, zero-knowledge secrets manager like the ones I recommended in Chapter 1.

3. Never send crypto to anyone without independently verifying that they are who they say they are, and that their wallet address is correct.

Slamming

Slamming is when a scammer switches a victim's service from one provider to another. Traditionally this practice targets utilities, insurance, landline phone service, and long-distance calling service, but it has expanded into more modern services such as Internet service providers, cellular service providers, and credit card processors (for merchants).[159] Slamming is unique in that it is almost exclusively perpetrated by actual employees (who are incentivized by commissions and/or sales quotas) of the companies that victims' service accounts are being transferred to. Here are a few of the companies that have been caught slamming in the recent past:

- SunSea Energy[160]
- Business Network Long Distance, Inc.[161]
- Communications Network Billing, Inc.
- Integrated Services, Inc.
- Multiline Long Distance, Inc.
- National Access Long Distance, Inc.
- Nationwide Long Distance Service, Inc.
- Network Service Billing, Inc.
- Systrum Energy[162]

---

159 https://www.allaboutadvertisinglaw.com/2018/08/fcc-tackles-slamming-and-cramming.html
160 https://6abc.com/slamming-electric-company-illegal-practice-salesman-action-news-troubleshooters/12186902/
161 https://www.fcc.gov/document/fcc-fines-seven-companies-12m-slamming-and-cramming-violations
162 https://whyy.org/articles/nj-sues-energy-suppliers/

- Palmco Power NJ
- HIKO Energy

Here are some extra measures you can take to make it more difficult to get slammed:

- Do not provide your personal information to any sales rep, or for surveys or contests.
- Do not reveal the names of your service providers (phone, cellular, Internet, electricity, water, etc.) to anyone over the phone or in writing.
- For businesses: do not allow anyone to "update" or "upgrade" or otherwise meddle with your point-of-sale devices.

If a credit check is not strictly required to establish service, and someone has enough personal information about you, then it's difficult to stop him or her from slamming you into a different service provider. The managers and customer service agents at the service provider that you've been slammed into may not be aware that one of their sales reps is opening fake accounts, and might therefore try to fight your attempts to close the account and get a refund. If you find yourself in this position, ask for proof of consent – a valid signature or a recording of a verbal agreement. If your signature or voice have been falsified or forged, then it's time to talk to the police or the FBI.

Fake Bank Accounts and Fraudulent Cross-Selling

Similar to slamming, bank sales representatives have been caught adding unwanted services to customer accounts, which is known as **cross-selling**. This is not illegal if you initiate or authorize it; for instance, if you have a checking account at a bank and respond to an offer to apply for that bank's Visa card. Unfortunately, scammy bank sales representatives who earn commissions from cross-sales or are required to meet unrealistic sales quotas are often glad to illegally use your personal information to secretly add services to your account, or to open new accounts in your name without your permission. It's bad enough that identity thieves want to use your personal data to open accounts in your name, but it's even worse when corporations do it.

As I explained in Chapter 2, Federal know-your-customer requirements make it impossible to avoid giving your bank your full name, date of birth, home address, and an ID number from a government-issued ID. Since you have no choice in the matter, you'd think that financial institutions would be held to the highest standards for information security, but they often violate their customers' data rights in various ways, and they rarely get more than a "slap on the wrist" as punishment. While it is illegal for bank employees to use your personal information to open accounts without your permission, financial institutions that collect personal information for KYC purposes are not generally forbidden from using it for marketing purposes, but they must provide the ability for customers to opt-out of information sharing with non-affiliated third-parties.[163] Details on how to opt-out are typically buried in the "fine print" of lengthy account agreement documentation.

In the past decade, five major banks have been found by the US Consumer Financial Protection Bureau to have opened a substantial number of fake accounts using people's personal data:

- TD Bank
- Bank of America
- Fifth Third Bank
- US Bancorp (US Bank)
- Wells Fargo Bank

Considering their past behavior – not just with fake accounts, but with other blatant anti-customer practices and regulatory violations over the past twenty years – it's probably safer for you to avoid using big corporate banks in general, and these banks in specific, if possible. That doesn't mean that smaller banks or credit unions aren't capable of the same or worse behavior. Regardless, you should spend a few minutes on due diligence for the banks you currently use (Wikipedia and DuckDuckGo are good enough for this purpose).

---

[163] https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

Aside from freezing your credit files as I advised in Chapter 1, the only other action you can take to help prevent fraudulent cross-selling is to opt-out of all pre-screened credit offers at this URL: `https://www.optoutprescreen.com`. This site is recommended by the US Federal Trade Commission (FTC), and it is safe to enter the personal information that it requests.[164] (But don't take my word for it – verify that claim for yourself!)

If your credit files are frozen at all three consumer reporting agencies, then it's much more difficult for other people to open a bank or credit account in your name. While it still might be possible for a particularly unscrupulous bank sales rep to open an account by manually bypassing KYC and credit-check requirements, the account would not be able to be reported to any credit agencies. Furthermore, this would raise red flags all over the place – within the bank's anti-money laundering compliance department, from the fraud detection systems at consumer credit agencies, from the Consumer Financial Protection Bureau, and possibly from one or more three-letter agencies.

By opting-out of pre-screened credit offers, you're making yourself a more difficult target for fake account fraud. These offers are generated based on information shared by credit reporting agencies. Even if your credit files are locked, banks can still obtain non-detailed information from your credit reports without your permission; this is known as a **soft inquiry**. Unlike hard inquiries, which represent a formal, documented request for a specific purpose, soft inquiries do not impact your credit score and are not typically recorded on your credit reports. By opting-out through the website mentioned above, you can prevent banks and non-bank credit card companies from obtaining any information about you through this method, and the less banks know about you, the better. However, any creditor or credit-dependent company that you currently have a relationship with (bank, credit card, line of credit, mortgage, insurance, and cellular service providers) will still be able to do periodic soft inquiries to validate that your basic information is still accurate and up-to-date.

[164] *https://consumer.ftc.gov/articles/prescreened-credit-insurance-offers*

Case Study: Wells Fargo

Among the commercial banks that were caught opening fake accounts to benefit from cross-selling schemes, by far the worst was Wells Fargo.[165] From a consumer perspective it's difficult to understand why a bank – especially one of the largest in the US at the time – would bother with such low-class high-risk fraud. The reason why it doesn't make sense to real people is: bank accounting is backwards from personal accounting. For instance, consider two different scenarios in which you borrow $1000:

1. Your friend loans you $1000. His personal balance sheet is now -$1000. This loan is a **liability** for your friend.

2. A bank loans you $1000 at 10% interest amortized over two years. The interest over the full term of the loan amounts to $107.48. Therefore the bank's balance sheet is now +$107.48, which is the difference between the loan principal (what you borrowed) and the principal plus interest at maturity (what you will pay back over 24 months). This loan is an **asset** for the bank; in essence, it bought $1107.48 for the price of $1000. If you miss a payment, the bank may also collect a late fee from you.

In other words: banks only make money when they lend it (or collect fees on it). Ideally they'd only lend to people who are certain to pay it back, because their entire system of accounting is based on the assumption that loans will be repaid on a prescribed schedule. When interest rates – which are primarily set by the US Federal Reserve and other national central banks – are low, however, assets (loans) are less profitable, so banks loosen their lending standards and take more risks on less-qualified borrowers so that they can issue more loans and collect more fees.

From a bank perspective the best customers are existing customers, because they already have a relationship with the bank, and the bank already knows their credit history. Therefore, banks put a lot of marketing resources into cross-selling new loans to existing depositors and debtors. If your mortgage is held by Wells Fargo, then you can expect that Wells Fargo will market its other products to you: checking and savings accounts,

---

[165] *https://abcnews.go.com/Business/timeline-wells-fargo-accounts-scandal/story?id=42231128*

CDs, credit cards, personal loans, home equity loans, etc. Each of these carries its own set of fees and interest payments.

In the early 2000s, Wells Fargo's CEO put tremendous pressure on branch managers to maximize cross-selling, and publicly bragged that the company's high stock price was due to its success with this scheme.[166] Each banker at every branch was expected to sell at least eight "financial products" to existing customers per day. Employees widely criticized this requirement as unrealistic, and as the sales pressure increased, so did turnover. If a banker did not consistently meet their sales goals, he or she was fired or pushed into resignation or retirement.

It's unclear when Wells Fargo employees started creating fake accounts to meet their cross-selling goals, but the first official record of fraudulent cross-selling activity was filed in 2002. Internal ethics complaints were, apparently, ignored.

Even when a cross-sale was legitimate, it was not always beneficial to the bank. For instance, bankers would push customers to take out a personal loan and then immediately repay it to avoid interest charges. Over time, the bankers who wanted to keep their jobs began to originate loans and open savings accounts and credit card accounts for customers without their permission, even going so far as to use false driver's license numbers and PINs to avoid customer knowledge and interaction. These practices continued until 2016, when there were at last enough consumer complaints against Wells Fargo to the Consumer Financial Protection Bureau, the Office of the Comptroller of Currency, and the City and County of Los Angeles to warrant a penalty.

Unfortunately that penalty was comically small: a $185 million fine, which was about 3% of the bank's quarterly profit. In addition, Wells Fargo fired about 1000 low-level employees. In response, many whistleblowers came forward, the news media reported extensively on it, and the public outcry was immense enough for the US Congress to hold hearings on the matter.

Here's the damage Wells Fargo did to people:

---

[166] *https://www.vanityfair.com/news/2017/05/wells-fargo-corporate-culture-fraud*

- At least 3.5 million fraudulent accounts were created, encompassing checking, savings, credit cards, and loans.
- Customers were compelled to pay a total of $2 million in bank fees.
- Customer credit scores were negatively impacted to varying degrees.
- Some customers, unaware of fees they owed on accounts they didn't open, were targeted by third-party collection agencies.
- Employees who were fired after reporting fraudulent cross-selling were blacklisted from employment at other banks.

As of 2023, Wells Fargo has been compelled to pay more than $3 billion in fines, settlements, restitution, and damages as a result of its cross-selling practices, and the Federal Reserve instituted a "growth cap" on the company of $1.95 trillion, which prevents it from expanding its assets beyond that level (though this was partially lifted in 2020 to assist with COVID pandemic relief).[167] Additionally, several major clients have severed their business relationships with Wells Fargo:

- The state of California
- The state of Illinois
- The city of Philadelphia, PA
- The city of Seattle, WA
- The Navajo Nation

Even after the fraudulent account scandal had been exposed, regulators, investigators, and lawyers continued to discover new fraudulent activity at Wells Fargo:

- Executives lied to shareholders about the timeline for lifting the Federal Reserve's growth cap, and the bank was ordered to pay $1 billion in restitution.

---

167 *https://web.archive.org/web/20200408210041/https://www.nytimes.com/2020/04/08/business/wells-fargos-coronavirus-small-business.html*

- Wells Fargo bankers also sold at least 15,000 fraudulent insurance policies through a partnership with Prudential Insurance, and re-opened insurance policies that customers had cancelled.[168]

- Customers were over-charged for foreign transaction fees, totaling more than $35 million.[169]

As I mentioned earlier in this section, Wells Fargo wasn't the only bank participating in fraudulent cross-selling; TD Bank, Bank of America, Fifth Third Bank, and US Bancorp (US Bank) were also caught and punished, and an investigation into multiple reports of account fraud at JP Morgan Chase was mysteriously terminated by the first Trump administration without comment from the CFPB or Chase.[170]

Considering these details, and the fact that big commercial banks are notorious for charging ridiculous fees, I encourage you to avoid any bank or credit union with a history of fraudulent account activity. Even if you're a pro at protecting your privacy, a greedy banker can still use your information to cause you stress and financial harm.

Extortion and Blackmail

The difference between extortion and blackmail is subtle: **blackmail** involves making a payment in exchange for preventing the release of private information, whereas **extortion** is broader in terms of what is exchanged and what is threatened. A victim of extortion may be compelled to take a specific action (such as voting for a specific candidate, purchasing something, or agreeing to perform a sexual act) under threat of some kind of harm, and may not have committed any crime or moral transgression; whereas blackmail victims typically pay money to someone to prevent them from revealing evidence of misdeeds. Both are crimes in the US, though their punishments differ by state and municipality.

168

https://web.archive.org/web/20161210235449/https://www.nytimes.com/2016/12/09/business/dealbook/wells-fargo-accusations-sham-insurance-policies.html

169 https://www.usatoday.com/story/money/2021/09/28/wells-fargo-pays-72-6-million-bank-customers-fraud-settlement-foreign-exchange/5896775001/

170 https://thecapitolforum.com/jpmorgan-chase-avoided-public-punishment-from-cfpb-under-trump-after-discovery-of-alleged-fake-accounts/

Along with theft of cash, extortion and blackmail are the oldest dirty-tricks in the book. In previous eras, the evidence required to blackmail someone would likely involve a handwritten letter, film negative, printed photograph, or video (film or tape). In today's world you can add several other digital mediums to the list: email, digital photographs and videos, documents, text messages, voicemail recordings, private messages and social media posts, search history, Web history, and location data.

These days blackmail largely takes the form of **sextortion,** where the perpetrator demands payment to avoid publicly exposing the victim's:[171]

- Sex video or nude digital photo that was either consensually recorded and stolen from a public or private data breach, or was secretly recorded by someone else.
- Membership of a pornography site, "hookup" service, or dating site.
- Sexual orientation, if the victim is not "out" to their friends, family, and co-workers.
- Attendance of or presence at a gay bar, pornography store or theater, swingers club, or some other event or location that implies a certain sexuality or sexual activity.

Men are about twice as likely to be sextortion victims as women, and the perpetrators are likely to be current or former romantic partners. However, women seem to be more at risk of having their nude photos and private videos secretly copied from their mobile devices, especially by repair technicians and device recyclers.

Sometimes the extortion is fake, even though it looks real. For instance there is a kind of email scam where the perpetrator will use some of your information stolen in one of the Internet's multitude of data breaches – usually your name, the username of one of your online accounts, and email address, but sometimes an account password as well – to send you an email claiming that you have been secretly recorded by your computer's webcam while visiting a porn site. In the email body and/or subject line, the scammer will reveal some of this stolen information to scare you into

[171] *https://www.upi.com/Health_News/2022/01/31/sextortion-online-blackmail-men-pandemic-study/1201643641232/*

thinking that they really do have something embarrassing about you that can be exposed, when in fact they do not.

Additional actions you can take to reduce your risk of digital extortion and blackmail:

- If you plan to go someplace that you don't want your friends, family, co-workers, and clients to know about, don't take your phone or smartwatch with you.
- Do not agree to be recorded while engaging in sex acts. If you do want to record yourself, avoid recording details that would identify you, such as your face, tattoos, birthmarks, and background items or images (such as a framed photograph, prescription pill bottle, diploma, or driver's license). If there are other people in the video or photo with you, you must have their permission to record them, and you should take the same precautions to protect their identity as you do for yours. If possible, insist on being the sole keeper of all such recordings.
- Assume that you are always being recorded in a public place.
- Ensure that your Web browser is not keeping a detailed history of the sites you visit, or cached pages and images from webpages.

Case Study: the Ashley Madison Data Breach

Cheating on a spouse is one of the classic blackmail setups. Someone records evidence of an affair, then threatens to release it to the public or to the victim's spouse unless they pay "hush money" to the blackmailer.

Now imagine that scenario scaled out to 30 million victims.

Back in the early 2000s a Canadian company called Avid Life Media (now known as Ruby Corp) launched a small portfolio of dating websites that catered to niche interests. Its flagship property was Ashley Madison, which specialized in helping married people find a partner for an illicit affair; its registered trademark slogan was: "Life is short. Have an affair."

A basic Ashley Madison membership was free, but male account holders couldn't interact at length with female members unless they purchased "credits" that granted a certain number of message responses, and/or a

certain amount of live chat time; female account holders never had to pay to send messages or participate in chats.

User privacy and – when requested – anonymity are of course paramount in this kind of business. Avid Life Media promised to safeguard its users' privacy, and made an effort to prove that its members' private information would not be revealed.[172] The Ashley Madison homepage prominently displayed icons representing a "Trusted Security Award," "100% Discreet Service," and "SSL Secure Site."[173] It put the word *discreet* in bold italic pink letters, and employed clever imagery throughout the site to project the illusion of discretion: photographs of models were blurred in contrived screenshots of member profiles and (possibly fake) customer testimonials, and the site's iconic homepage featured the lower half of a female model's face with a shushing finger over her lips. However, those promises and credentials were hollow; the company wouldn't let members delete their accounts without paying a "full delete" fee, essentially holding their private information hostage. Even if someone paid for deletion, though, Avid Live Media still secretly kept a record of every paying customer's full legal name and home address.

In July of 2015, Avid Life Media employees received a demand letter (in the form of an image that had been forcibly displayed on their workstation screens) from a hacker group calling itself "Impact Team."[174] In it, the hackers claimed to have copied all user account data – including names and addresses of former members who thought they'd paid to have all of their information removed from the company's records – plus images (some of them nude), member conversations, financial records, source code for the site's software, company bank account details, personal information about employees, and years of internal company emails. It was arguably the most comprehensive corporate data breach in history.

Bizarrely, the perpetrators did not want money. Rather, citing the company's false promise to delete user accounts after they'd paid (and the amount of money – $1.7 million – that Avid Life Media had collected in "full delete" fees), and credible allegations of facilitating prostitution and

---

172 https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/
173 https://krebsonsecurity.com/wp-content/uploads/2015/07/ashleymadison.png
174 https://krebsonsecurity.com/wp-content/uploads/2015/07/impactteam-580x657.png

human trafficking through its dating sites, "Impact Team's" only demand was for Ashley Madison and one of its sister sites, Established Men, to be shut down forever. If the company did not comply within one month, then the hackers threatened to publish all of the data they'd stolen. To prove that they weren't lying, they provided a sample of the stolen data. As far as extortion demands go, this one was exceptionally mild.

With a reported annual revenue of $115 million in 2014, and plans to take the company public with an IPO (initial public offering) later in the year, Avid Life Media's leadership chose to take their chances and ignore the threat.[175] In retrospect – considering what the company's management knew about their dishonest business practices, and the potential fallout from all of their user data being publicly revealed – this was an incredibly bad idea. Exactly 30 days after the demand letter was delivered, "Impact Team" publicly released 60 gigabytes of the data they'd stolen, minus some things they felt were irrelevant or uninteresting, such as pedestrian emails among rank-and-file employees, and pictures of men's genitalia.

The publication of the stolen data was an absolute nightmare for Avid Life Media and many of its Ashley Madison customers, to the point that it would certainly have been better for the company to have complied with "Impact Team's" demands:

- Analysis of the Ashley Madison data and backend source code revealed that the company was lying about a lot of its user metrics and activity:
    - The company had created a massive number of fake female profiles for chatbots that would attempt to coerce men into paying for credits to respond to them.[176]
    - More than 84% of accounts were men.
    - Less than 1% of women's accounts had any significant activity.

[175] https://www.smh.com.au/technology/ashley-madison-made-a-lot-of-money-and-created-very-few-affairs-20150824-gj6er7.html
[176] https://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924

    - The fraudulent "full delete" scheme came to light, which generated a class-action lawsuit.

- User account details – including exclusively-reserved IP and email addresses – were revealed that put many Ashley Madison users in jeopardy:
    - Public servants in local and federal US government.
    - Active-duty members of the US military.
    - People who live in countries that criminalize adultery, such as Saudi Arabia.
    - Politicians and "reality TV" stars, most notably: Josh Duggar, Hunter Biden, Jionni LaValle, Josh Taekman, Jeff Ashton, Jason Dore, and Sam Rader.
    - Sex workers who used the site to find clients.
    - Members of the clergy.
    - An Alabama newspaper editor published the names of every local Ashley Madison member within the paper's coverage area.
    - Innocent people who never used Ashley Madison, but their email address had been used by someone to create an account as a prank.

The consequences were dire:[177]

- Avid Life Media faced many lawsuits and fines totaling tens of millions of dollars, its revenue dropped substantially, and it was forced to spend millions of dollars on security upgrades to its infrastructure.
- Several exposed Ashley Madison users committed suicide.
- Scammers used the publicly-leaked Ashley Madison data to attempt to blackmail its current and former members.

---

[177] *https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0*

- Avid Life Media's planned IPO, in which it expected to raise $200 million in capital, was cancelled.
- The CEO was forced to resign.

Thus far I've spoken of Ashley Madison in the past tense, but despite the many painful consequences of its management's carelessness and negligence, Ashley Madison never went offline for any substantial length of time. In fact, during the overwhelming negative publicity over its data breach in 2015, company representatives claim that there were still more than 100,000 new user signups per day.[178]

Ruby Corp – as Avid Life Media is now known – promises that this time it's different: you can do an actual "full delete" of your private data, there are no chatbots on fake user accounts, and they finally have that "information security" thing handled. Today the site has more than doubled since its data breach, with over 60 million members.

Some people never learn; don't be one of those people. If you want to have an extramarital affair, arrange it offline where your personal data can't be captured and used against you in the future.

Ransomware

By using a trojan horse known as **ransomware**, digital thieves can encrypt your computer's hard drive and offer to send you the encryption keys after you pay a ransom (usually in cryptocurrency). But even if the attackers honor the deal, the data they encrypted should always be assumed to be stolen; if someone can execute ransomware on a computer, then he or she can also copy all of the personal data on it and sell it on the Dark Web.

There are more than 600 million ransomware attacks in the world each year. Local governments and small/medium-sized businesses are particularly vulnerable to ransomware attacks because they are known to have access to sufficient funds to pay a worthwhile ransom; and are notorious for using old and insecure hardware and software, and for failing to implement proper information security controls. However, ordinary people can be targeted, too.

---

178 https://venturebeat.com/business/ashley-madison-affairs-in-the-time-of-coronavirus/

Ransomware is usually enabled by users downloading and executing a trojan horse, or by clicking a link to a malicious website, though attackers will also attempt to use brute force tactics. More sophisticated ransomware schemes involve exploiting an unpatched remote software vulnerability, most often in a computer's operating system, back-end server software, or network hardware.

Here are some additional actions you can take to prevent yourself from being a victim of ransomware:

- Immediately apply any available security updates to your devices' operating systems and all programs installed on them.

- If you are running a server from your home or business, ensure that the firmware is up-to-date on all of your network equipment (router, hub, modem).

- Only use a currently-supported version of your computer's operating system. Older computers may not be compatible with newer operating system releases, and they can be left vulnerable to remote attacks if they are no longer supported. If your computer hardware cannot run the latest major release (not smaller "point releases") of Windows, OS X, or Linux, then it should be taken offline and safely disposed-of.

- Backup your most important data to removable media (USB drive, CD, DVD, or Blu-Ray) at least once per year, preferably every six months. If you want to be maximally secure against fire and theft, then store your backups in a fireproof safe or bank safety deposit box.

- Deploy a secure automated cloud backup solution for important documents and other often-used files, and enable 2FA for it. This is not only a precaution against ransomware, but also against hardware failure. If your computer dies or your house is destroyed in a fire, then you should not lose access to your most important digital assets.

Spam (email), Spam (snail mail), Spam (telephone and text), and Spam (door)

We've come to think of "spam" as unwanted email, but in the modern world it can take a few other forms:

- **Junk mail**: printed marketing communications sent by US mail or other delivery services.
- **Robocalls** and **junk text messages** sent to your cell phone.
- **Door spam**: printed marketing materials affixed to, slipped under, or jammed into the front doorway of your home, office, or business.

Spam, in its many forms, can only exist when spammers know your contact information. Spamming is usually cheap, but it's never free; it always costs something to create and send a massive amount of anything – even email messages. So at the very least a spammer needs to have a valid destination in the form of an email address, mailing address, or phone number. Sometimes they may not know exactly who is at that destination – such as with door spam and junk mail addressed to "current resident" – but most of the time spammers have at least a decent idea of whom they're targeting.

One of the most insidious forms of non-scam spam is **remarketing**, where companies use your personal information to repeatedly show you targeted ads across several sites, services, and apps.[179] Typically this involves recording your Web search and website activity history with cookies and tracking scripts embedded in apps, webpages, and emails, then using various technologies and information sharing practices to associate it with your demographic and contact information. From that point forward, every time an online advertiser is able to identify you, you will be targeted with remarketed ads and spam. Your remarketing data profile may even be sold to third-parties without your knowledge or permission. Most of the time this applies to ads on websites and in mobile apps, but remarketing can also lead to any kind of spam. For instance if you're signed into a Google account and you use Google to search for *wedding dresses,* then click through to various results, thanks to remarketing technology you may find a printed wedding dress catalogue in your physical mailbox a week or two

[179] *https://support.google.com/google-ads/answer/3124536?hl=en*

later (this actually happened to one of this book's contributors who wasn't engaged to be married – he was merely using Google to develop a search exercise for another book: *Google Power Search!)*

The best way to reduce spam is to limit the personal information you provide to corporations, and to take the precautions I've already explained in previous chapters. In Chapter 6 there are some further actions you can take to opt-out of marketing communications.

Real-World Harm

When your personal information falls into the wrong hands, the consequences are not always isolated to the virtual realm. Motivated attackers can easily cause harm in the real world as well.

The issues documented in this section are only possible if an attacker knows where the victim currently lives and/or works, and is able to connect their online handles / accounts / player IDs / usernames to their real names. The process of publicly connecting someone's personal information with their (usually anonymous) online identity is known as **doxing** (or **doxxing**). I have specific advice for how to handle a doxing incident in Chapter 6.

SWATting

This is the practice of calling a police department (often with a spoofed phone number) to falsely report a terrorist threat or a serious violent crime in progress, with the hope that the police will respond blindly with extreme force in the form of a militarized SWAT (Special Weapons And Tactics) team that is primed for violence. The victim's house or office can be invaded by armed and armored police without warning, often with deadly consequences for the occupants, pets, neighbors, and guests. In documented swatting cases, the perpetrators rarely have what most people would consider to be a "good reason" for attacking someone: wanting to take possession of the victim's social media handle, anger over an online match in a video game, or simply to indulge their sadistic tendencies.[180]

Without the assistance of Internet trolls, the cops occasionally get it wrong all on their own by arriving at the wrong address for a legitimate call or

[180] *https://www.kaiserslauternamerican.com/swatting-cyber-awareness/*

(more commonly) planned drug raid. There have been several high-profile cases of SWAT teams breaking down innocent people's front doors, destroying their personal property to perform a search for drugs or weapons, shooting their dogs, and sometimes shooting the occupants, or being shot by the occupants – all because of a mistake in reading a street name or house number. There's a lot that could be said here about the militarization of police forces, excessive use of force, and draconian anti-drug laws, but I don't want to get too political.

Here are some ways you can protect yourself from swatting:

- I usually tell you *not* to make your personal information easier to find, but this is one important exception. Help emergency responders find the correct address for your home by ensuring that your street number is clearly printed on the front of your house (follow the rules provided by your local municipal government and/or homeowner's association), and also your mailbox (if it's on your property) and, if permitted, the curb next to your driveway. If you're in an apartment or condo, make sure the correct unit number is printed on or next to the door.

- Never reveal your real name, phone number, or any other personal information in an online forum, game, livestream, voice or text chat service (such as Discord or Ventrilo), or any other virtual public community. Don't use real photos of yourself for game profiles.

- If you're trying to become a professional streamer or social media influencer, you'll be safer if you use a pseudonym instead of your real name for your public persona. This won't completely protect you from swatting or other forms of harassment, but it will make it more difficult for low-effort trolls to reach you outside of your public platforms.

- If you believe that you may become a target for swatters, check with your local police department to see if they have an anti-swatting program that you can register for. Since swatting is almost universally perpetrated via a voice phone call, you may be able to add your name, street address, and phone number to a private list that officers will consult before responding to a threatening or suspicious call.

- Enable the **Emergency Location Service** feature on your mobile devices. Turning it off will *not* prevent your cellular service provider from sending geolocation data to emergency responders when you call 911 or any other emergency number, so you may as well turn it on so that the EMS dispatcher can get more accurate coordinates. As anti-swatting techniques and procedures improve, features like this will make it much easier for dispatchers and police to quickly determine whether an emergency call is legitimate. Unlike caller ID, Emergency Location Service technology cannot be spoofed by a remote attacker.

- Swatting is almost exclusively the domain of violent or addictive online multiplayer game communities. If you play games like those, do not engage in "flame wars" or other personal rivalries with trolls, griefers, cheaters, people who are "extremely online," or anyone who seems to have a level of commitment to an online game that a normal, mentally healthy, well-adjusted person would reserve for a family or career.

Robbery and Vandalism

As I said back in the "The Cost of Lost Trust" section in the Introduction to this book, strangers are overwhelmingly not a threat to our safety, and in fact are generally far more willing to help us than harm us.[181] So in the offline world, unless you are in a particularly dangerous place, you rarely have to consider the intentions of the people you meet and socially interact with, and unless you're doing something that you don't wany anyone to know about, or you're a public figure such as a celebrity or politician, you don't usually have to worry about someone recording or documenting everything you do and say.

However, as I explained in Chapter 3, *unrecorded information* can still be used to influence, manipulate, harass, or steal from you. Even if you are good at protecting your personal information, your friends, family, neighbors, and co-workers may not be. Salespeople, con artists, thieves, violent activists, and foreign intelligence agents are skilled at casually fishing for personal information through conversation and observation, then using it

[181] *https://news.stanford.edu/2022/09/08/asking-help-hard-people-want-help-realize/*

to their advantage: to build rapport, identify a weakness or vice, or plot a property crime such as vandalism or theft.

Remember the movie *Home Alone,* where the thieves knew exactly when the wealthy homeowners in a certain neighborhood were going to be away for the holidays, and how they would make it look like they were home by setting a timer on their outdoor lights? That's a perfect example of the kind of information a thief or vandal would find valuable. Most home invasion robberies are not blind, door-to-door fishing expeditions; rather, they are the result of critical information falling into criminal hands, starting with the knowledge that a home or office contains something worth stealing, such as cash, drugs, firearms, or expensive jewelry.

Vandalism is also often the result of criminal knowledge of personal information, though this is probably a lot less complicated than you're imagining. For instance if you attend an Arizona Cardinals home game and leave a Seattle Seahawks flag flying from your car's radio antenna, then you can expect that it won't be there (or it will be torn to shreds) when you return to the parking lot, and possibly your antenna might be missing as well. Whomever steals and/or destroys that flag and defaces your car is probably someone who would not vandalize any other car in any other context, but by learning of your football team loyalty in a hostile environment, he or she made a spur-of-the-moment decision (possibly motivated by alcohol) to vandalize your car.

You can of course be indignant over this because "it's a free country and I have the right to do whatever I want," but unless you secretly enjoy being enraged and making car insurance claims, it benefits you, your family, and your community to avoid behavior or activity that a reasonable person would consider antagonistic or provocative toward strangers – especially in your absence. The law is often not on your side when you intentionally provoke or antagonize someone into harming you or damaging your property.[182]

Sometimes vandals and thieves are extremely angry at their victims on a long-term basis, and commit property crimes purely out of pent-up jealousy or revenge. For instance politicians, journalists, and the employees and (especially) managers or owners of companies that engage in ethically or morally questionable practices, and/or negatively impact people's lives

[182] *https://www.law.cornell.edu/wex/provocation*

can find themselves targeted by vengeance-seekers in various ways, including murder, physical assault, kidnapping, home invasion, and sabotage or defacement of their homes and vehicles. People can also be upset with a company because of the actions of one particular employee; fast food restaurants, for example, are notorious for customer service issues that later turn into violence and vandalism.

Here are some examples of companies and institutions that may be more likely to be targeted for vandalism, revenge theft, and violence:

- Laboratories that use animals for testing drugs or consumer products
- Factory farms / animal agriculture
- Women's healthcare providers (even if they don't offer abortion services)
- Religious organizations and places of worship
- Public schools
- Government buildings
- Political party and political activism offices
- Health insurance providers
- Police stations and vehicles
- Victim support and social service providers
- Banks
- Law firms
- Post offices
- Foreign embassies
- Stores that cater to specific ethnic groups

Also at risk are any individuals who identify (or can be identified) as a member of any ethnicity, religion, nationality, or sexuality that is specifically targeted by hate groups or terrorist organizations.

Here are some actions you can take to make yourself less vulnerable to targeted property crimes:

- Don't be provocative toward strangers, especially when they know where your car is parked or where you live or work, or if they're serving or preparing food or drinks for you.

- Don't post about upcoming vacations, medical procedures, or events on social media. Thieves prefer low-risk theft. If a thief knows that you're not going to be home on July 4th because you posted on Facebook that you'll be out at an all-night Independence Day party, then you may as well leave the front door unlocked and put some snacks out for him or her on the kitchen counter. If you must post on social media, do it after you're already home, not before or during the event.

- If you own a safe – no matter what is in it – do not tell anyone about it, and instruct your family not to tell anyone about it either. The presence of a safe implies that it contains something worth stealing.

- Don't tell anyone that you own guns. Broadcasting the fact that you have guns is exactly as self-destructive as telling everyone that you have a large amount of cash. If you make it publicly known – on your t-shirt, hat, yard sign, bumper sticker, or social media post – that you protect your property with your .45 revolver and/or AR-15 rifle, then thieves know exactly who to steal guns from. <u>You aren't Clint Eastwood.</u> Most gun crimes are committed with weapons that were obtained legally, then either illegally resold by or stolen from legitimate law-abiding gun owners; and 80% of school shooting massacres are committed with stolen guns.[183] <u>Owning a gun is secret information;</u> no one should ever know about it – even (perhaps *especially)* your children. Concealed-carrying a gun is also secret information; you must take care to not "show" (present an obvious gun bulge or other evidence that you are carrying a firearm) or "tell" (be seen adjusting a holster, or literally tell someone that you're carrying a firearm). Regardless of whether the law allows it, if your safety and security are important

[183] *https://www.npr.org/2023/02/10/1153977949/major-takeaways-from-the-atf-gun-violence-report*

to you, *never* open-carry a firearm – you may as well open-carry a bundle of $100 bills. A hardened criminal will not be intimidated by your gun; rather, he or she will see it as a highly valuable prize to be taken from you via a violent surprise attack.

- Your beliefs and affiliations should be as private as possible. Without completely stifling your creative self-expression, try to be a "grey rock" in public – an uninteresting target for people who are looking for trouble. Protecting your privacy means being less expressive about your political beliefs, religion, income level, and social status. The US constitution may guarantee that Congress cannot restrict your political speech, but it does *not* guarantee that you won't be the target of politically-motivated thugs who have nothing to lose and don't care about going to jail. Don't antagonize activists with yard signs, flags, t-shirts, hats, or bumper stickers. No stranger needs to know that you think that the 2020 election was stolen from Donald Trump, or that you are a staunch Zionist, or that you support the Confederacy, or that you are in favor of trans-gender bathroom rights. These issues may be of critical importance to you personally, but expressing them blindly to unknown and/or unseen strangers in public will change no one's mind; it will only make you vulnerable to violent activism and crimes of opportunity. Psychopaths are always looking for "good reasons" to victimize others, so the last thing you want to do is provide a violent person with an excuse for giving you the ill-treatment he or she feels that you "deserve." Vote with your ballot, not your public persona; for optimal privacy, safety, and security, the only correct venue for expressing politically sensitive issues is the polling place.

Litigation and Legal Defense Problems

Crime is not always the sole domain of criminals. Innocent people are regularly arrested and sometimes even tried and convicted for crimes that they did not commit. More commonly it's possible for an otherwise law-abiding citizen to unwittingly break laws that they know little or nothing about. For instance, giving a ride to a hitchhiker could lead to a human trafficking charge; feeding a wild animal can be a state or federal wildlife offense; and an unmaintained oak tree in your back yard could fall onto your neighbor's house during a storm and cause serious injuries and extensive property damage that you could be held liable for.

Information is *everything* when it comes to legal issues. Not just evidence, but also testimonies, depositions, and data that can be obtained from service providers. The foundational principle of the US justice system is that one is innocent until proven guilty, but the reality is that innocent people can and do fail to adequately prove their innocence before a judge or jury, most often because of a combination of unskilled defense lawyers, false or ambiguous eyewitness accounts, forced or manipulated confessions, and circumstantial evidence.

If you are ever formally charged with a civil or criminal offense, then you'll be glad you took every precaution to protect your personal data. In a trial, every piece of relevant obtainable information about you will be used against you by opposing counsel: social media posts, location data from any mobile app that collects it, GPS history from your vehicle, electronic payments for toll roads, receipts for purchases, cellular tower triangulation data, the contents of text messages and emails, credit card transactions, video and photo recordings of you (or someone who looks like you) from public and private cameras, Web search history, and cryptocurrency transfers.

On the other hand, if you are the plaintiff in a case, you'll want to document as much as possible to prove that you have the legal grounds and standing to bring your case before the court. If you're a defendant and you are truly, unambiguously innocent, some of the data that could be used against you can also exonerate you. For instance if you're accused of robbing a liquor store on the west side of town, your location-tracking data, photos or check-ins on social media, and credit card transaction data could prove beyond a reasonable doubt that you were in fact at a movie theater on the east side of town when the robbery occurred.

In a perfect world we would allow ourselves to be privately tracked for evidential and historical purposes, and have absolute control over the selective release of that information. Unfortunately we are very far from that utopia; we don't even know which corporations might be recording information about us at any given time, and what they will eventually do with it. But, as always, there are extra steps you can take to limit the information that may someday be used against you:

- Whenever possible, do not use any mobile app that broadcasts your location to other app users or third-party service providers. Don't let your smartwatch or fitness-tracker record or broadcast

your location. Be extremely wary of social media apps that broadcast not only your location, but also your identity, such as Strava, Runkeeper, Zwift, and Instagram.[184] I recommend never using any app that lets strangers know who and where you are, but if you must use one of these apps, then try to configure them to not record or publish any personal or private information.

- Whenever an app requests to access your location data, opt to grant it manually on a one-time (per-use) basis. Ridesharing apps and driving directions apps (such as Google Maps and Waze) require location sharing, but you don't have to grant always-on blanket permission.

- If you are formally interviewed by the police for any reason, do not talk to them without your lawyer present, even if you are certain you've done nothing wrong. Everything you say to a police officer is officially recorded and will be used as evidence if necessary. Regardless of innocence, if you give the cops enough information, and they can't find a more qualified suspect for a particular crime, then you could be arrested and detained.

Case Study: Google Snitch

(The material in this section is based on an excerpt from *Google Power Search,* by Stephan Spencer)

Google and Apple track the location of all of the mobile devices that use their operating systems. As I explained in Chapter 3, while Apple's current policies (which may change at any time) prohibit the company from storing a device's location history, Google retains a substantial amount of fine-grained location data in a product it calls **Sensorvault**.[185] Even if you're an iPhone user, if you use Google services on your Apple devices, then Google is recording at least some location information about you.

Law enforcement officers and private citizens can request access to current or past device location data for a wide range of purposes, from **geofencing warrants** (legal demands for personally-identifiable location

184 https://www.kaspersky.com/resource-center/preemptive-safety/fitness-tracker-privacy
185 https://www.apple.com/legal/transparency/pdf/requests-2022-H1-en.pdf

data of mobile devices that were present in the vicinity of a crime) for criminal investigations, to court-ordered wiretaps of suspected terrorists, to subpoenas in civil divorce cases.

Government agencies have long been able to obtain basic device tracking data from cellular service providers (such as T-Mobile, Verizon, and AT&T), but the kind of location data that Google and Apple can provide is much more accurate and detailed than old-fashioned cell tower triangulation coordinates. When police or FBI agents are having a difficult time coming up with reasonable suspects or witnesses after a major crime is committed, they will obtain a geofencing warrant which compels Google to give them any Sensorvault data relevant to the crime scene. This gives the cops a topographical view of the precise paths mobile device-holders took through a crime scene area before, during, or after the commission of the crime. Typically this data is anonymous at first; if the cops want to go one step further to identify any of the people who own those devices, then Google and/or Apple will provide the identifying personal information (full name, phone number, and potentially other information) that corresponds with each of those devices.

Sometimes police will ask for geofencing data without a warrant, such as in smaller cases where a mobile device is stolen (to track the mobile device and hopefully recover it), or to investigate claims that a mobile device (or user account) was used for fraudulent or illegal purposes. Aside from restrictions imposed by the law in those jurisdictions, it is up to the individual judgement of Apple and Google executives to determine how, when, and to whom such data will be provided.

While Sensorvault data can be invaluable for catching dangerous criminals in some circumstances (such as when the FBI used geofencing data to identify participants in the January 6, 2021 insurrection and riot at the US Capitol building), it can also lead police down a garden path.[186] If you happen to be in the vicinity of a crime and are the only person carrying a cell phone, then you might be considered a prime suspect in a crime that you aren't even conscious of.[187] There have been several documented cases where innocent people have been harassed and falsely accused of crimes

[186] *https://www.msnbc.com/deadline-white-house/deadline-legal-blog/geofence-search-warrants-jan-6-rcna67515*
[187] *https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants*

based solely on data obtained from geofencing warrants. Here are two particularly awful examples:

- In 2018, Arizona cops used Google Sensorvault data to arrest Jorge Molina as a suspect in a murder, despite there being no motive or any non-Sensorvault evidence, and having an alibi with several credible witnesses.[188] Eventually Jorge was exonerated and released, but irreversible damage had already been done: he lost his job because the police arrested him while he was at work, he had to spend a week in jail, and his car was impounded for evidence and then repossessed for lack of payment. It isn't totally clear why the Google Sensorvault data led to his arrest, but it had something to do with his mother's ex-boyfriend sometimes borrowing his car, and Jorge occasionally checking his messages from other people's Android devices.

- Zachary McCoy used an app called RunKeeper to track his physical activity, which often included biking three laps around his Gainesville, FL neighborhood. RunKeeper uses Google location services, and Google records all of that activity in its Sensorvault database. One morning in January 2020, Zachary received an email from Google's "legal investigations support team" informing him that they would give the personal data stored in his Google account to a local police department unless he went to court to ask a judge to block the request.[189] Unable to get any actual legal investigation support from Google's "legal investigations support team," he looked up the court case number printed in the email, and found only a one-page police report about a 2019 burglary of an elderly woman's home about a mile from the house he rented with two roommates. Zachary did not know the woman in question, had never visited her house, and didn't even know anyone who knew her or had any knowledge of the alleged burglary some 10 months prior. Terrified of being arrested and charged with a crime he didn't commit, Zachary asked his parents to use money from their savings account to hire a lawyer to help exonerate him. The lawyer they hired was able to convince the state attorney to rescind the

188 https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html
189 https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

> geofencing warrant, and eventually remove Zachary McCoy from consideration as a suspect to the alleged burglary. Despite causing him undue expense, neither Google nor the Gainesville Police Department reimbursed Zachary's parents for his legal fees.

Google isn't the only threat in situations like this. Any kind of mapping service or fitness tracker could collect data about you that law enforcement could use against you, even if you haven't committed a crime. Apple claims that it currently does not retain geofencing data, though it still can track a device's current whereabouts, and will provide that information to law enforcement when compelled by a warrant or court order.

Stalking, Social Catastrophe, and Suicide

As I mentioned in the Ashley Madison and Google Snitch case studies, the publication of private data – even if it's just an email address, bike route, or credit card transaction – can have serious consequences for your relationships and career. Beyond extortion and embarrassment, though, stalkers, self-styled "social justice warriors," "Internet sleuths," and "anti-racists" are just as capable of causing mayhem for ordinary people by weaponizing mobile apps and social media sites, even when they're completely innocent. Below are case studies that further illustrate this point.

Case Study: Stalkerware Leads to a Triple Murder

In 2013 a man named Luis Toledo suspected his wife, Yessenia Suarez, was having an affair, so he secretly installed a mobile app called SMS Tracker on her Android smartphone, which gave him access to all of her text messages and photos in real-time. When data from SMS Tracker revealed that his wife was indeed cheating on him, Luis murdered Yessenia and her two children. Luis Toledo was arrested, convicted, and sentenced to three consecutive life sentences for his crimes, but the people who created, marketed, and sold the SMS Tracker app were not held legally responsible for enabling him.[190]

---

190 *https://web.archive.org/web/20230520002943/https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html*

Ostensibly SMS Tracker was designed to help parents monitor their children's smartphone usage, but it was easy for users and reviewers to imagine using this app for other purposes, as revealed by this review on the Google Play Store: "I would recommend if you think your partner is cheating." The company that sold SMS Tracker – Gizmoquip – even quoted a glowing review that anticipated the unintended consequences of using it: "I'm kinda sad to know that apps like this might signify the moment you stop trusting someone in your family and the subsequent implication for that. You can use a trial version for seven days, but think carefully about it huh?"[191]

SMS Tracker is no longer available on the Google Play Store, but not because these kinds of apps were banned by Google; rather, the company seems to have gone dark in 2014 and ceased supporting it. As of April 2025, there are many Android apps available that do the same things as SMS Tracker. How many crimes have they enabled?

Case Study: Strava Data Made An Innocent Man Into a Target for Vigilantes

Social fitness apps like Runkeeper, Strava, and Zwift (among many others) ostensibly help you track your outdoor exercise patterns and help you connect with a community of locals who share the same activities. But when an app helps people connect to strangers, it reveals critical data about them that can be used for harm.[192] You do not need these kinds of apps to meet other people who share your interests or activities. Even if you have made a new friend or two through a "social fitness" or social media app, the potential for future harm far outweighs any past benefit.

For example, consider the case of marketing executive Peter Weinberg, who used Strava, a social fitness app for cyclists, to record his uneventful journey on the Capital Crescent Trail in Maryland on June 2, 2020.[193] Two days later, he began to receive abusive and threatening messages through various social media and social networking apps, most notably LinkedIn. At first he wrote them off as spammers or scammers, but eventually they

191 https://gizmoquip.com/index.php#about
192 https://www.bbc.com/news/technology-52978880
193 https://nymag.com/intelligencer/2020/06/what-its-like-to-get-doxed-for-taking-a-bike-ride.html

were numerous and serious enough that Peter decided to look into it further. A growing number of tweets and direct messages on his seldom-used Twitter (X) account accused him of assaulting a child and of being "racist." He was baffled. He'd never harmed a child, nor done or said anything that could be construed as "racist."

One of the abusive tweets directed at Peter juxtaposed a photo of him in his bike helmet – a "selfie" he'd taken and shared publicly on social media – with a blurry image captured from a "viral" video of someone else who'd been accused of assaulting a child and an adult who'd been posting and distributing fliers in support of George Floyd – a black man accused of passing counterfeit money who'd recently been killed by police officers in Minnesota, causing a nationwide outrage against police violence against impoverished black men – near the Capital Crescent Trail.[194] Peter was still confused; he'd had no interaction with anyone on his bike ride, and felt that the man in the blurry video looked nothing like him aside from a similar pair of sunglasses and a similarly-colored bike helmet, but for some reason a multitude of self-styled "social justice warriors" were so certain that it was him that they felt entitled to say things like this:

- "You assaulted a little girl and other innocents because of your political beliefs."
- "Hey so are you the piece of shit who assaulted a child in Maryland today on the bicycle trail?"
- "Hey you racist bitch….we're coming for you."
- "You deserve to pay."
- "Ur going down u disgusting piece of shit."
- "Nice job assaulting a small child today. You need to be fired from your job immediately."
- "YOU UGLY RACIST BITCH."

194

https://www.reddit.com/r/Strava/comments/gzbd3r/can_anyone_from_strava_clear_up_the_peter/?rdt=58723

When one social media vigilante told Peter that the police were coming for him, he called the Maryland-National Capital Park Police Department to find out what was going on. It turned out that someone from the department had put out this call for leads on Twitter on June 2, along with the blurry photo from the "viral" video of a cyclist assaulting the George Floyd activists:

> *"We are seeking the public's assistance in identifying the below individual in reference to an assault that took place this morning on the Capital Crescent trail. Please contact Det. Lopez with any information."*

June 2 was the day that Peter had ridden the Capital Crescent Trail. After talking to the police, however, it was revealed that there was an error in that tweet. The department posted this correction:

> *"Correction, the incident occurred yesterday morning, 6/1/2020."*

Whoops! Peter Weinberg had been working from home all day on June 1 and had many witnesses (and corroborating app data) who could verify that he was in Zoom meetings during and around the time of the alleged assault, so the cyclist who attacked the George Floyd activists could not possibly have been him. But that follow-up tweet had only a tiny fraction of the reach of the original tweet that incited the "social justice" mob to find and extra-judiciously punish the unknown bike-riding assailant. Once a mob is formed and motivated, it's nearly impossible to force all of its constituents to cease exacting their individual interpretations of vigilante justice on whomever they deem worthy of targeting. The Maryland-National Capital Park Police Department's follow-up tweet was almost universally ignored.

Even after Peter was publicly exonerated, the vast majority of the people who threatened and abused him did not put the same level of effort into repairing the damage as they'd put into causing it. Still, Weinberg responded en masse with this message on Twitter: "We must align in the fight for justice and equality - but not at the cost of due process and the right to privacy and safety." I couldn't agree more!

Case Study: Redditors Crowdsource Harassment of a Suicide Victim's Family

Harassing people on social media is never the right thing to do, no matter how much you believe they may "deserve" it. Even if the person being targeted is unquestionably and absolutely guilty of a crime or non-criminal transgression, being abusive toward them online or over the phone is cowardly, crass, and doesn't make anything better for anyone; worst of all, sometimes you'll end up harming innocent people.

On March 16, 2013, 22-year-old Sunil "Sunny" Tripathi disappeared.[195] He'd suffered from depression, and couldn't imagine a viable future for himself. He stopped showing up for classes at Brown University, and didn't respond to phone calls or text messages. His family reported him missing, and organized a public search effort to help find him in both Providence where he studied, and in his hometown of Boston. The campaign to find Sunny included posters, fliers, news media interviews, and eventually a Facebook page dedicated to the cause. Unfortunately they didn't receive any useful leads.[196]

On April 15 – three weeks after Sunny's friends and family began their search effort – two terrorists detonated homemade bombs at the Boston Marathon, killing three people and injuring 281 others. A dozen law enforcement agencies at the local, state, and federal level immediately began searching for the perpetrators, but before they could provide any useful and definitive information to the public, rumors and misinformation on social media poisoned the narrative. Various Twitter (X) users, in particular, published false leads and wild speculation; the national news media for some reason largely abandoned its ethical standards and began reporting some of that misinformation on TV and in newspapers.

It would be three days before the FBI would release photos of the two suspects, though they had not yet been identified.[197] While this may have generated some useful leads for the FBI, it also made the rumors and misinformation far worse. A group of Redditors decided to create a

---

[195] https://www.npr.org/sections/codeswitch/2016/04/18/474671097/how-social-media-smeared-a-missing-student-as-a-terrorism-suspect
[196] https://en.wikipedia.org/wiki/Suicide_of_Sunil_Tripathi
[197] https://www.theatlantic.com/national/archive/2013/04/reddit-find-boston-bombers-founder-interview/315987/

subreddit to crowdsource the identity of the terrorists by combining pieces of information from various law enforcement agencies, social media accounts, media organizations, and witnesses. Despite an effort by the moderators to remove posts containing personal information, a number of innocent people were publicly accused of being terrorists:[198]

- Abdul Rahman Ali Alharbi, a 21-year-old college student from Saudi Arabia who was injured in the bombing. Police stormed and searched his apartment while he was still in the hospital being treated for shrapnel wounds; he was threatened with deportation by various members of the Federal government (who later retracted their threats), and his roommate was harassed by news reporters.[199][200]

- Salah Eddin Barhoum, a 17-year-old high-school track star who was watching the race. *The New York Post* published a photo of him and his track coach on its front page with the headline: "BAG MEN." Salah's friends notified him of his status as a media-crowned suspect; in a panic, he asked a friend to drive him to a state police station so he could turn himself in. The police informed him that he was not a suspect.

- "Michael Mulugeta," who doesn't actually exist as far as anyone can tell. A Twitter (X) and Reddit user named Greg Hughes claimed to have heard the police mention this name as one of the bombing suspects over the Boston police scanner.

- From that same scanner-listening Twit came a report (which was later proven to be false) that the name of the other suspect was Sunil Tripathi.

Prior to the scanner misinformation, a woman on Twitter claimed that a missing classmate of hers looked like one of the terrorists: Sunil Tripathi. This claim was amplified by journalists, pundits, and others on social media, and seemingly corroborated by the false report of hearing it over a

---

198 https://theweek.com/articles/465307/4-innocent-people-wrongly-accused-being-boston-marathon-bombing-suspects
199 https://news.yahoo.com/report-saudi-national-ruled-suspect-boston-marathon-bombings-050427325.html
200 https://theweek.com/articles/465460/boston-marathon-tragedy-should-new-york-post-apologize-blaming-innocent-saudi-national

police radio. There is no good reason why Sunny stood out as extra-suspicious to the news media and their social media "sources;" but being vaguely middle-eastern- or west-Asian-looking (his parents were from India) certainly did not help in a culture that had been conditioned to assume that all terrorists were Muslim (as it turns out, the actual terrorists were in fact radicalized Muslims from Kyrgyzstan), and the fact that he had gone missing a few weeks before the bombing made it easier to speculate about him in his absence.[201] Regardless, this was enough "evidence" for the Reddit vigilantes to anoint Sunil Tripathi "Marathon Bomber #2," and then unironically congratulate themselves with the now-infamous phrase, "We did it, Reddit!"[202]

As the misinformation about Sunny spread through both the news and social media, legions of people who assumed that he was one of the bombers went to the Facebook page that his family had established to help find him, and posted extremely abusive messages not only about him, but directly to his family as well. For several hours they struggled to delete hateful messages as they were posted, but eventually had to shut off all comments on the page, which also prevented anyone from posting potentially useful information about Sunny's whereabouts.

That evening, Tamerlan Tsarnaev and his brother Dzhokhar went on another terror rampage on their way to set off bombs in New York City. After two shootouts, a car chase, and a manhunt, they were both caught, and publicly named as the *actual* and *official* Boston bombing suspects. Even as this was happening, Sunny was still being falsely named as one of the Boston bombers on social media.

A few days after the Tsarnaevs were caught (Tamerlan died after being runover by his brother in a stolen car; Dzhokhar was shot, but survived in custody), on April 23, Sunny's body was discovered floating in a river in Providence. Even after being publicly exonerated, social media users continued to speculate about Sunil Tripathi. Had he been alive during the terrorist attack? Was he murdered by the Tsarnaev brothers? Did he commit suicide after seeing his name smeared with false accusations and his family publicly attacked on Facebook? Eventually the *actual* and *official*

---

201 *https://web.archive.org/web/20131128065048/https://www.thewire.com/national/2013/04/reddit-find-boston-bombers-founder-interview/64455/*

202 *https://knowyourmeme.com/memes/we-did-it-reddit*

determination by the medical examiner was that he'd been dead for some time – likely long before the bombing – and had committed suicide by drowning.

One of Reddit's managers later apologized to the Tripathi family in a blog post.[203]

203

https://www.reddit.com/r/OutOfTheLoop/comments/34oirt/what_was_the_we_did_it_reddit_incident_and_who/

Chapter 5: The Indirect Consequences of Surrendering Your Data

If you're careful and know how to protect your privacy, you can easily avoid most of the direct harm that can result from carelessly sharing (or refusing to safeguard) your personal information. *Indirect* harms, however, are much more difficult to avoid because you're never clearly confronted by them; they're invisible, and in most cases you won't even know that you've been affected. If you're aware of them at all, you're probably actually pleased with them because they are most often disguised as something that you believe you benefit from, need, desire, identify with, or enjoy. The frightening part about this is: you've probably been coerced or manipulated into feeling that way.

Imagine you're invited to play a card game like poker, blackjack, or gin rummy, with a $20 buy-in. As soon as you sit down at the table, one of the other players offers to give you $5 if you'll lay your cards face-up on the table for the entire evening. "Hey," you think (because you are terrible at gambling), "Five bucks for free! Fifteen more and I break even. I'll take it." But under these conditions it would only be possible to win a round if you were dealt a perfect hand, and your opponents would cut their losses

early by folding or forfeiting as soon as they saw that you had better cards. There are in fact some card games that are played similar to this, such as the poker variants Mexican Sweat, Blind Man's Bluff, and Night Baseball, but the rules are configured so that every player has an equal advantage. If you were the only player at the table whose cards were visible to the others, it would be nearly impossible for you to finish the evening with more chips than you started with. After the final round, you'd be lucky to cash-in any chips at all, and the player who offered you $5 at the beginning would walk away with most of your stack.

You could argue that this is an effective strategy for hedging your $20 bet by limiting your losses to $15, but it also guarantees that you'll lose money. Why would you pay $20 to receive $5? By focusing on the free $5, you've willingly given up not only on your initial $20 buy-in, but also any money you would have won if the other players couldn't see your cards. This scenario may seem silly, but it's exactly what many people do every day without realizing it; they trade their valuable privacy, agency, and dignity for minor comforts, conveniences, and discounts of lesser value without understanding the consequences.

Personal data collection is often part of a reciprocal process; you feed your information to companies, and they attempt to give you their personally-targeted marketing messages or influential political propaganda in return. To illustrate the potential danger this can pose to you and your family, consider the parable of "The Eagle Wounded by an Arrow" from *Aesop's Fables:*

> *An Eagle was soaring through the air when suddenly it heard the whizz of an Arrow, and felt itself wounded to death. Slowly it fluttered down to the earth, with its lifeblood pouring out of it. Looking down upon the Arrow with which it had been pierced, it found that the shaft of the Arrow had been feathered with one of its own plumes. "Alas!" it cried as it died, "We often give our enemies the means for our own destruction."*

While this is a good bit of general wisdom, the likely original version of that story (which predated Aesop by at least a century) is more useful as

an allegory for how surrendering your personal information can come back to harm you later. Here's how the older version ends:[204]

> *So the eagle, pierced by the bow-sped shaft, looked at the feathered device and said: "Thus, not by others, but by means of our own plumage are we slain."*[205]

Put more plainly: a feather that the eagle discarded while preening itself ended up being a critical component of the weapon that killed it. In the literal sense, there isn't much of a lesson here; for birds, *preening* is a necessary and instinctual maintenance activity that resets the cohesiveness of good feathers, and facilitates growth of new feathers by removing old ones that are too damaged to repair – not unlike the human practice of washing, brushing, and trimming one's hair. But this is an allegory, so we must interpret it metaphorically. In human terms, *preening* and *plumage* refer to aspects of vanity, not of routine personal hygiene. By making our vanities obvious to all, we reveal our greatest weaknesses, and therefore give our adversaries the tools to undermine and manipulate us. Corporations gather our discarded feathers (our likes, shares, follows, photos, ad clicks, purchases, preferences, Web search queries, email opens, and the personal information that we freely share online), then use them to fashion the arrows (advertisements, social media posts, "sponsored articles," "special offers," recommendations, spam, and press releases) that will most effectively wound our vulnerabilities so that they can exploit our weaknesses for their benefit.

The more you "preen," the more arrows you help to create. For instance if you give Facebook all of your personal information, then Facebook will target you with ads that are highly specific to you, and alter what you are most and least likely to see in your content feed, including which capital-F Friend posts, Likes, and suggested Friends, Pages, and Groups are shown. Some of this is in service to Facebook's desire to drive engagement and keep you scrolling through your feed as long and often as possible (no matter how unhappy it makes you feel), but mostly it is in service to the

---

[204] *https://en.wikipedia.org/wiki/The_Eagle_Wounded_by_an_Arrow*

[205] *https://books.google.com/books?id=tBKLAwAAQBAJ&dq=Babrius++++%22Eagle+wounded%22&pg=PA194#v=onepage&q=Babrius%20%20%20%20%22Eagle%20wounded%22&f=false*

advertisers that have paid Facebook to show you their ads and promoted posts, which will attempt to entice you to buy something, influence your vote in an election, alter your opinion of a public figure or foreign nation, or create discord by enraging you with disinformation and political propaganda. This is not specific to Facebook; the same paradigm applies to all platforms and services that sell targeted advertising.

Aside from entering information and clicking buttons on social media apps, here are some other ways that we fletch the arrows that slowly destroy our productivity, mental health, social connectedness, national identity, and economic prosperity:

- Responding to surveys
- Officially registering or affiliating with a political party
- Donating to charities, schools, alumni associations, fraternities, clubs, or religious organizations (I'm not saying it's bad to donate to worthy causes, but you must be mindful of if and how those organizations protect your information, share it with others, use it to continually solicit donations from you, and how you can opt-out, all of which is covered in Chapters 6 and 7)
- Entering a contest or promotional giveaway
- Participating in retail discount / rewards / loyalty programs or services
- Installing retail store apps on your mobile devices
- Clicking or tapping on an online ad
- Signing up for a newsletter or mailing list
- Accepting anything claiming to be "FREE"
- "Registering" a product purchase with the manufacturer
- Connecting your social media accounts to third-party sites, apps, or services
- Giving mobile apps permission to constantly access your GPS location

- Using your real name as a publicly-viewable user account for a site, app, game, or service
- Applying for credit
- Searching Google or YouTube while signed into your Google account

It seems almost ridiculous that these everyday (and sometimes necessary or virtuous) activities could possibly lead to significant harm, but that's what makes them so dangerous. In this chapter I'll show you how, individually or in aggregate, these data collection methods can enable retailers, lobbyists, media producers, and foreign agents to manipulate you for their benefit without your knowledge: you will subconsciously choose certain brands when buying products that you've never bought before; you'll find that you've developed new opinions on companies or politicians, but you won't know exactly why; you'll develop a longing to buy a certain product without anyone trying to convince you; and you'll notice that your monthly spending has increased in ways that are difficult to quantify. In the worst scenarios, you will find yourself mired in addictions or gambling; or you may find yourself developing negative opinions of people who are of certain races, nationalities, religions, genders, political parties, or sexual orientations; if left unaddressed, these toxic feelings may someday boil over into self-destructive behaviors and/or acts of hate and violence toward others.

Overspending

The oldest and most common side-effect of surrendering your personal data to corporations is overspending; they want you to buy their stuff, and they have devious ways of coercing and influencing you into giving your money to them.

Think about your local grocery or convenience store. If you're like most people, then your interactions with these places are quick, straightforward, and transactional. You go to the store with a list, and typically don't deviate from it; or you only go for one thing like a gallon of milk or a sixpack of beer. You already have preferred brands in mind for most of the products you intend to buy, or perhaps you'll buy the only brand available. You enter

the store, go directly to the familiar aisles and shelves, grab the items you need, pay, and leave.

What do you suppose would happen if you took a more leisurely shopping approach, though – if you went to the convenience store "just to see what they have today?" Unless you have superhuman willpower or left your wallet in the car, the chances of you leaving the store without buying anything are almost nil because every item in every store is designed and placed for maximum influence (in fact, companies often pay retailers a premium to place their brand-name products in more visible or accessible locations within the store). The moment you start paying attention to everything around you in a store, you begin subjecting yourself to those influences. Even if you're someone who eats healthy food as a rule, if you actively browse the junk-food aisles in a grocery store, you're going to at least be strongly tempted to buy something that violates your diet, and if you are feeling tired or depressed, you're even more likely to succumb because junk food promises (falsely!) to improve your mood.

Brick-and-mortar stores are limited in the scope of their influence. Typically each store has certain demographics in mind when its layout is designed. That's why malls were such a big retail success for so long (and why they were disrupted by online retailers like Amazon, but I'll get to that in a moment). Each store in a mall is narrowly focused on a specific demographic such that each person in a family or a group of friends who visit the mall and walk through it are eventually drawn to one or more storefronts, sometimes to the chagrin of the other people they're with.

Now imagine that everyone in your life got together to use what they know about you to build the perfect store just for you, containing only the things you like, no matter how obscure, rare, expensive, unrealistic, or varied they may be. At first that may sound like a great idea – everything you want, and nothing you don't! – but it wouldn't take very long to recognize this as a Faustian bargain. Most of the stock in this specialized store would be of the "rare treat" variety: your favorite flavors of ice cream, freshly-made pizza from that obscure Italian takeout place in your hometown that closed down 20 years ago, every movie you wanted to watch but missed, clothes that make you look and feel great right now (not five years ago or "someday when I lose weight"), the exotic supercar from the poster on your wall when you were 12. This store would ruin your life. You'd be morbidly obese and massively indebted in a matter of weeks, all because a

retailer had access to a bonanza of your personal data. Sounds like an episode of *The Twilight Zone,* doesn't it?

This scenario is not as unrealistic as you might think. In fact there are several powerful technology companies that are actively applying this same "perfect store" philosophy on the Internet. Amazon is the most obvious example – the entire site is highly personalized to each visitor based on their prior purchases, search terms, page views, current location, and "wish list" items – but Google, Facebook, X, and LinkedIn are also trying to learn everything they can about you so that they can show you ads that are likely to influence you to buy or believe something. Again, this may seem like a good thing. After all, aren't irrelevant ads really annoying, especially when you're forced to look at or listen to them? But if every ad you see on the Internet is specially made to appeal to you, then you'll eventually end up in the same condition as you would after visiting your "perfect store" – unhealthy, unhappy, and broke. The evidence (in the form of increasing levels of obesity and consumer debt in the US) suggests that many people have already succumbed to the influence of greedy retailers and advertisers.[206][207]

The Retail Information Loop

Anyone who's ever spent time in a flea market, pawn shop, bazaar, or souk (particularly in a non-Western nation) has participated in or at least witnessed the ancient art of haggling. If prices are listed at all, they are typically over-valued so as to enable the shopkeeper to lower them to make deals. Friends and family will of course get the lowest prices, but everyone else has to be individually judged. If you're a skilled haggler (and not a snappy dresser), you can probably score a better deal on a wheel of cheese than, say, a foreign tourist or wealthy-looking businessman. However if the shopkeeper doesn't like you for whatever reason, he may refuse to offer you a deal – or even refuse to sell to you at all. A Jewish woman in a Muslim souk is unlikely to score any deals.

In the Western world there is rarely any haggling in a retail setting; the price on the pricetag is the cost, no matter who you are. This is not merely a matter of convenience; it is also the foundation of universal equality in a capitalist system. The pricetag on a can of beans on a supermarket shelf is

[206] *https://www.newyorkfed.org/microeconomics/hhdc*
[207] *https://www.cdc.gov/obesity/data/adult.html*

the same for black people and white people, men and women, immigrants and citizens, children and adults, Jews and Muslims. (Though, as I'll explain shortly, digital pricetags on store shelves now enable stores to instantly change the price of any item.)

All of that goes out the window when you buy something online. By monitoring real-time market trends and collecting personal data, online retailers and service providers are able to alter both the digital pricetags and the ostensible availability of every product and service for every individual customer. If they know you will pay a higher price than someone else, then your pricetag will be higher than theirs. Here are some real-world examples:

- Uber and AirBnB charge different rates for different people on different dates and at different times of day.[208][209]

- Airlines use their frequent flier programs and customer histories to offer different people differently-priced fares for the same seats on the same flights.[210]

- Discount travel sites like Travelocity, Expedia, Hotwire, Hotels.com, and Priceline use a similar dynamic pricing scheme, but also use other data such as how long a visitor has been browsing fares on the site, how many times a user visited their site, and the external links that referred those visitors; they also alter the availability of airline seats and hotel rooms to make them appear more scarce than they really are.[211]

- Orbitz was caught charging 20-30% more for hotel reservations if the visitor was using an Apple computer.[212]

---

[208] *https://www.forbes.com/sites/forbestechcouncil/2019/01/08/dynamic-pricing-the-secret-weapon-used-by-the-worlds-most-successful-companies/*
[209] *https://www.uber.com/en-GH/blog/uber-dynamic-pricing/*
[210] *https://simpleflying.com/dynamic-pricing-airlines/*
[211] *https://www.nbcnews.com/better/lifestyle/travel-website-you-re-using-says-there-s-only-1-ncna1073066*
[212] *https://www.wsj.com/articles/SB10001424052702304458604577488822667325882*

- Amazon adjusts the prices of items millions of times per day based on its massive collection of customer and supplier data.[213]

- Wal-Mart and Kohls use digital pricetags that can be adjusted instantly.[214]

- Target, Staples, and Home Depot adjust the pricing in their mobile apps based on customer data.[215][216]

In most brick-and-mortar retail stores (with the exception of those that use digital pricetags), pricetags are still printed and therefore unchangeable based on who's thinking of buying the items on the shelves. That doesn't mean that you'll always pay what the pricetag says; instead of haggling, the deal-seekers of the Western world constantly try to pay less than the sticker price by way of promotional sales, manufacturer's coupons and rebates, special discounts, subscription services, contests, referral bonuses, and rewards programs, all of which are targeted at specific groups of people through various means. Unfortunately those schemes and sales are designed to encourage overspending, so they generally have the opposite effect: ultimately you end up spending more money.[217][218][219]

Obviously no store or manufacturer wants to take less money from you for no reason. Traditionally, coupons, rebates, and promotional sales were delivered through ads in print and broadcast media. You'd clip a coupon, mail in a rebate postcard, or "mention this ad for a discount." These were purely methods of letting the store or manufacturer know that their ads were effective. Ad salespeople promised them that their ads would reach a certain number of people who fit certain demographic categories, and coupons and promotional discounts not only proved whether their ads

---

213 https://qz.com/157828/amazon-changes-its-prices-more-than-2-5-million-times-a-day
214 https://www.retailcustomerexperience.com/news/walmart-deploying-vusion-for-digital-shelf-strategy/
215 https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514
216 https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data
217 https://www.bloomberg.com/opinion/articles/2023-05-11/credit-card-reward-programs-can-be-a-predatory-trap
218 https://www.thepennyhoarder.com/debt/credit-card-rewards-costs/
219 https://www.mentalfloss.com/article/78017/5-ways-coupons-actually-make-us-spend-more-money

were working, but also served to get customers in the door where in-store marketing techniques would hopefully encourage them to buy more stuff.

All of that is largely "old hat" in the age of digital advertising and mass data collection. In fact tech-savvy retailers have been using personal data to target ideal customers for decades. They know exactly who they want to see their ads, and when, where, and how they want them to be experienced. Consider this *New York Times* article quote about pregnant women from Andrew Pole, who helped develop Target's customer data marketing technology:

> *"We knew that if we could identify them in their second trimester, there's a good chance we could capture them for years. As soon as we get them buying diapers from us, they're going to start buying everything else too. If you're rushing through the store, looking for bottles, and you pass orange juice, you'll grab a carton. Oh, and there's that new DVD I want. Soon, you'll be buying cereal and paper towels from us, and keep coming back."*[220]

The article goes on to cite an instance where a man complained to a Target store manager that his teenage daughter had received store coupons in the mail for baby clothes and cribs. The man was angry because he believed that Target was trying to encourage his daughter to get pregnant so that it could sell more stuff to her. As it turns out, though, his daughter actually *was* pregnant. By collecting the girl's purchase history and other personal data, Target's marketing algorithms knew about her pregnancy before her parents did. By analyzing the buying habits of women who were known to be pregnant, Target could predict not only a pregnancy, but which trimester the mother was in and the baby's approximate delivery date. You could reasonably expect Target to know that someone's expecting a baby if they buy newborn baby clothes and accessories, but the frightening part about this is that most of the products in the algorithm only peripherally suggested pregnancy. For instance: calcium, magnesium, or zinc supplements; unscented soap; large packages of cotton balls; hand

[220] *https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html*

sanitizer; and washcloths. This news story is from 2012; just imagine what Target can do today.

By using personal data such as your demographics (age, sex, income level, etc.), Web and app search history, purchase history, social media participation, current and previous mobile device location telemetry, the services and service providers you use (such as cellular, home Internet, video and audio streaming, club memberships, etc.), and your employment details (title, field of expertise, employer), advertisers can more effectively target you (and by that I mean *specifically* you) with ads when and where you are most susceptible to influence. I've already mentioned how this will lead to various forms of spam and junk mail, but it can also alter the things you are exposed to on social media and anywhere data-driven ads or sponsored content are shown.

Beware Your Emotions

While the allegory of "The Eagle Wounded by an Arrow" applies generally to all of the topics in this chapter, it is especially useful as a ward against being manipulated into overspending. The marketers at Target knew that pregnancy is a major life event that makes people extremely vulnerable to influence. They also knew that if they could just get an expectant mother into one of their stores, they could use in-store marketing techniques to manipulate her into buying more than she intended to.

Consider some other major life events that could make you vulnerable to influence:

- Death of a loved-one
- Death of a pet
- Being involved in a lawsuit
- Being arrested or charged with a crime
- Divorce
- Proposing marriage
- A serious injury or illness (for you or a loved-one)
- A car accident

- Buying or selling a home
- A change in employment (promotion, layoff, or working for a new company)
- Starting a business
- Graduating from high-school or university
- Being accepted to a university
- Retirement
- Moving to a new place

Now let's take it down a notch, and consider some less unusual but still emotional situations:

- Doing your taxes
- Paying your insurance premiums
- Managing chronic pain
- Paying for a major car repair
- Renewing a lease
- Leaving for or returning from a vacation
- Receiving a "special assessment" from your building or homeowners association
- Change in relationship status (breaking up, or meeting someone new)
- Your favorite sports team wins or loses the national championship

You could probably come up with at least 20 more scenarios like these. They can be either stressful or joyful – it doesn't matter, because either way you are in a state of mind that makes you vulnerable to suggestion and influence. To understand what that influence looks like, ask yourself how you know the answers to these questions:

- How much should an engagement ring cost?

- What kind of computer does a creative person use?
- If a package absolutely, positively has to be there on time, which shipping company would you choose?

It's likely that you've answered: three months' salary, a Mac, and FedEx. These are myths created by corporate marketing campaigns to influence people to overspend. The De Beers Diamond Consortium's "three months' salary" meme is so powerful that many people actually believe it is a genuine cultural tradition. Most of the world's greatest creative minds existed before Apple made its first computer, and Macs don't do anything that cheaper alternative devices can't. FedEx has consistently been less reliable than one or both of its main competitors during the peak (holiday) season; perhaps the company has determined that it's cheaper to run ads to the contrary instead of improving the efficacy of its logistics operations.[221]

From now on, I urge you to classify all of the above-listed life events – and any others you can think of – as private information. Telling your friends that you're getting married isn't going to harm you, but posting about it on social media or creating a wedding registry at a retail store will set the marketing forces of the world against you. If you feel that this is too big a sacrifice (you do want wedding gifts, after all), then you should at least commit to being mindful of the fact that retailers and service providers will be sending you spam in various forms, and targeting you (and the people you're connected to on social media) with online ads and mobile app notifications. If you know they're out to get you, then you're better enabled to negate their influence.[222]

Shutting Down The Perfect Store

Aside from all of the standard advice I've given thus far, such as using a privacy-focused Web browser, using a VPN whenever you're online, and refusing to give up personal information whenever possible, here are some things to consider for reducing or eliminating the "perfect store"

---

[221] Source: https://www.supplychaindive.com/news/ups-leads-peak-season-on-time-delivery-rate-fedex-shipmatrix/639852/
[222] https://www.theatlantic.com/technology/archive/2023/09/retailers-consumer-tracking-data-personalized-ads-influence/675181/

influences on the Internet so that you have a better chance of being happier, healthier, and wealthier in the future:

- Avoid using products and services that have integrated ads that you cannot block with a Web browser or VPN.

- Avoid using ad-supported businesses in general, especially "free" news media sites. Good, high-quality things always cost money; "free" things may cost no money upfront, but you could end up ultimately paying a higher price in terms of being exposed to toxic ads and disinformation, and having your personal information harvested to be used against you. Remember: "FREE is not good for me."

- Never click on an ad, anywhere, ever. If you happen to see something in an ad that interests you, then go to the company's website – don't click on its ad. Every ad click is, to some degree, a harvesting of your available personal data. You already know how to shop for something you want; you don't need the assistance of ads. Also, as I explained in Chapter 3: sometimes ads are scams or phishing attempts.

- Condition yourself to have "ad blindness." Whenever you see something that looks like an ad, especially if it's designed to grab your attention, tell yourself: "This is just hype. I don't want to see it."

- When possible, don't buy anything from notorious data-collectors, most notably Amazon, FlipKart, and AliExpress. If there are alternative online stores that you can buy from without creating an account (usually this is referred to as **guest checkout**), use them instead. There are often better – albeit not always ostensibly cheaper – alternative retailers that have more customer-friendly business models. Costco, for instance, derives most of its profit from membership fees, not from sales of goods, services, or customer data.

- If you do sign up for an account at an online retailer, reveal as little information about yourself as possible – you don't need to specify your age, gender, or other non-essential details – and if those fields are required, give them dummy information (unless you're buying

age-restricted products that are required by law to validate your age and identity), and don't let them store your payment information.

- Be mindful of your emotional state when you're tempted to purchase something. Are you under stress? Are you filled with joy, sorrow, worry, or regret? Would you buy this stuff if you were feeling content, calm, and rational? Will you be okay if you don't buy this thing right now?

- Before you post something on social media, imagine it being fed into a giant datacenter full of customer information that will be used against you in the future. Instead of posting to social media, consider calling or texting your friends and family with good or bad news.

- All sales, discounts, and promotions are tricks to get you to overspend, as are rewards and loyalty programs. It's usually better to buy what you need when you need it; if you wait for a special sale, you're likely to end up spending more than you intended.

Self-Harm

Marketers and propagandists play a long game; they don't want just one sale or one vote, they want you to keep coming back for more, and the way they achieve that is by convincing you that you're unhappy, incomplete, in danger, or "missing out" on something. Social media platforms show you not only ads, but also content that you're likely to engage with – comment on, Like, share, follow, etc. The more you interact with social media, the more stimulating the recommended content will be; at first it will be amusing or interesting, but eventually it will escalate into media that offends, shocks, shames, stresses, or enrages you.

Regardless of whether it's a retail ad or a sponsored post or a suggestion to read or watch something provocative, the information that marketers and propagandists feed us for their own benefit is universally and unequivocally unhealthy for humans to consume because it is designed to make us feel scared, angry, inferior, flawed, or incomplete. Marketing campaigns seek to exploit people's existing fears and insecurities; unscrupulous marketers will try to inspire new insecurities in people who otherwise wouldn't have them, then they sell the solution.

If you're in good health, are financially and socially stable, and are secure in your career, relationship, and home, then advertising probably doesn't have much effect on you unless it's rational, straightforward, and informs you of the features of a new product or service that you are already interested in buying without being manipulated by beautiful models, bright colors, celebrity endorsements, and earworm jingles. If that's as far as the exploitation went, then we'd probably be okay – ads can be blocked, skipped, or muted – but social media companies like Google (YouTube), Meta (Facebook, Instagram, Threads), and X constantly develop and use increasingly complex engagement algorithms that collect our personal information and use it to create custom media content that can reach us in ways that are uniquely effective. Facebook, for instance, has over 100 data points on each of its users, including their disposable income, expenditures, and the value of their home; this data is made available to advertisers for targeting purposes, and is used internally to drive engagement.[223] If you have cancer or are engaged to be married, Facebook's algorithms can reasonably calculate how long you have to live or how expensive your wedding will be. They also know that negative emotions inspire engagement.

Meta's social media platforms are particularly evil in this regard. Leaked internal memos from 2018 revealed that Facebook managers were aware that its algorithms were rewarding outrage by promoting content that created negative responses from users, and CEO Mark Zuckerberg refused to address it.[224] In 2019, an internal research team at Facebook published these conclusions in a slide presentation:[225]

- "We make body image issues worse for one in three teen girls."
- "Thirty-two per cent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse."

---

[223] https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data
[224] https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215
[225] https://www.theguardian.com/technology/2021/sep/14/facebook-aware-instagram-harmful-effect-teenage-girls-leak-reveals

- "Teens blame Instagram for increases in the rate of anxiety and depression. This reaction was unprompted and consistent across all groups."

And in a US Senate hearing in 2021, former Facebook manager Frances Haugen testified that Facebook and Instagram "harm children, stoke division, and weaken our democracy."[226]

When we have self-destructive feelings and thoughts, psychiatric therapy can help us overcome them by reprogramming our brains through professional guidance, with the goal of learning to thrive on healthy beliefs and productive habits. Commercial and political propaganda is psychiatric therapy's evil twin because it does the exact opposite: it influences us to change our self-image in order to alter our behavior for someone else's benefit. The propagandist seeks to make us believe that there is something deeply wrong with us or our environment, and only the proposed solution (buying or subscribing to something, donating money, voting for a particular candidate or party) can make it right. Consider the immortal words of the renowned 20th century British philosopher Sir Michael Philip Jagger:

> *I can't get no satisfaction.*
>
> *When I'm driving in my car, and a man comes on the radio telling me more and more about some useless information that's supposed to fire my imagination,*
>
> *I can't get no satisfaction.*
>
> *Cause I've tried and I've tried and I've tried.*
>
> *I can't get no satisfaction.*

[226] *https://www.scientificamerican.com/article/facebook-whistleblower-testified-that-companys-algorithms-are-dangerous-heres-why/*

When I'm watching my TV, and a man comes on to tell me how white my shirts can be, but he can't be a man because he doesn't smoke the same cigarettes as me,

I can't get no satisfaction.

The state of *dissatisfaction* with one's life is exactly what propagandists seek to exploit – or if it doesn't yet exist, to instill it in us, and to continually exacerbate it. Once we are in that state of mind, we begin to look for relief. Over a period of time, we become receptive to solutions to our malaise that we would never have considered previously, no matter how expensive, silly, or destructive they may be to us, our family, and our community. But after someone's bought the suggested item, donated money, or voted as advised, the negative feelings don't go away; the cycle continues.

Propaganda can be indirect. Consider how Red Bull markets its sugar-and-caffeine drinks:

1. Television commercials that feature cartoon characters becoming super-powered after drinking a can of Red Bull, then proclaiming: "Red Bull gives you wings," in a whiny, annoying, sing-songy voice that is difficult to forget.

2. Videos on the Internet that show an athlete, race car driver, or stunt performer sipping from a can of Red Bull before winning a competition or successfully executing a dangerous stunt.

In both cases the point is to make viewers believe that drinking Red Bull will make you perform better than you otherwise could. In order to be receptive to these ads, we must be convinced that we are not good enough just as we are. A healthy, well-adjusted person will not respond to this kind of advertising unless the content of the ad – or another form of propaganda – causes them to doubt their adequacy. Once a negative self-belief has taken hold, it opens us up to a wide variety of similar messaging from other sources, all of which seek to convince us that we are defective unless we spend our time, attention, money, and votes on the products, companies, topics, and politicians that will make us whole again. And to be perfectly clear: consuming mass quantities of caffeine and sugar ala Red Bull is *not* healthy, nor is the belief that one cannot perform well without drinking it.

The subsections below explain some of the methods that marketers and propagandists use to manipulate us into making unhealthy and self-destructive choices.

Rage-Farming

Consider for a moment how much time you spend each day engaging with various forms of media that cause you to feel angry, stressed, offended, or shocked. Did you seek out this material, or was it shown to you while you were looking at or for other things?

More than anything else, modern Western social groups are defined by the perception of a common threat to their collective safety and prosperity, whether that be political or social.[227] Affection for one's "team" is not sufficient to prove loyalty to the group; one must also express a baseline level of hatred for the "other team" and its beliefs, behaviors, and culture in order to qualify as a true compatriot. Marketers and propagandists know this, and create media content to stoke specific fears and reinforce prejudices (**rage-farming**); this conditions people to be receptive to advertising, and it is greatly exacerbated when people freely reveal which "teams" they are on by registering for a political party, donating money to a political campaign, clicking on online ads, and Liking or Following accounts and pages on social media.

While all social media services encourage rage-farming in various ways and to various degrees, perhaps the best example is Quora.[228] Originally it was designed (by two former Facebook employees) as a "free" crowdsourced question-and-answer service where registered users could ask questions and hope to get a variety of expert or celebrity responses. At first the company had no revenue model, but eventually it began selling targeted ads integrated with the site's content; presently Quora's main source of income is advertising (again: <u>if you aren't the customer, then you're the product</u>), though it also gates some of its premium expert-authored content behind a paywall for subscribers who pay monthly fees to access it (some of the proceeds are then paid to the expert authors who have the

---

[227] https://www.theatlantic.com/ideas/archive/2024/01/cultural-pessimism-america-self-fulfilling-effects/677261/

[228] https://www.theatlantic.com/technology/archive/2024/01/quora-tragedy-answer-websites/677062/

highest level of engagement).[229] Because its service fundamentally relies on users providing personal information to prove the depth of their expertise – their name, email address, topics of interest, occupation or field of study, location, educational history, professional experience, and any other profile information users willingly provide (such as their photo) – Quora is able to offer its advertising clients a wealth of targeting options. Even worse: while an abbreviated view of Quora's content often shows up in Web search results, the bulk of every post is gated behind a social media (Facebook or Google) or email login; if you choose to connect your Google or Facebook account to Quora, it can access some personal data from, and share data with, those data collectors.

Social media cannot survive without engagement; in Quora's case, this means users posting questions and answers on a regular basis. In the beginning this was easy, but when questions began to be redundant and answers largely had not changed from previous posts, engagement began to drop, especially among well-known contributors. At that point – and up until 2023 – Quora began paying some of its users to generate questions that led to high levels of engagement. It's easy to see how this business model led to rage-farming: the more provocative the question, the more engagement it generates, which leads to more ad views and more ad clicks. Here are a few examples of provocative Quora questions (you can decide for yourself whether they're genuine curiosities, or contrived to generate negative attention):

- "I caught my son playing his Xbox at 12:00 in the morning on a school night. As a result, I broke his console and now he won't talk to me. How can I tell him that it is his fault?"
- "My husband accidentally pushed our 4-year-old daughter off the 40th story window out of anger. How do I prevent my husband from being sentenced to jail? He doesn't need that hassle."
- "Was Hitler actually a nice guy in person?"

Quora sends emails or push-notifications containing questions like these to its users with the hope that they'll generate enough of an emotional reaction to click through to the site, engage with it by posting an

[229] *https://www.investopedia.com/articles/investing/041916/how-quora-works-and-makes-money.asp*

impassioned reply, and view and click on some ads. The more information you give to Quora, the better enabled its algorithms are to expose you to questions that are likely to generate this kind of reaction.

It's worth repeating: Quora isn't alone in this practice, it's just the most obvious and egregious example. All "free" sites – not just social media – that survive on engagement and advertising eventually turn to clickbait and rage-farming to increase revenue. In some cases it is intentional, but even when it's not, engagement algorithms will always promote whatever gets the most attention regardless of why, and that is almost universally something that will make you upset (on an individual basis as determined by your personal data, or as a known member of a group that has certain beliefs and prejudices).

How Media Consumption Affects Your Health

We are hard-wired to respond quickly and unconsciously to negative stimuli; stressful situations naturally attract our attention above all else, and we remember them more often and more completely than experiences that generate positive emotions. Consider, for instance, your memories of watching footage (or if you were there at the time, your actual experience of observing) the World Trade Center terrorist attacks of 2001; compare that with your memory of the most recent time your favorite sports team won a championship. Or think about when you got married, and analyze the depth and accuracy of the events and experiences that were happy and went as planned, and the things that went wrong or caused stress. When we tell stories from our past, they are most often framed as victory at the end of a string of hardships, or as a string of successes that improbably led to defeat. Stories where everything went perfectly as planned aren't nearly as interesting – not just to other people, but also to ourselves.[230]

Unless you live or work in an unsafe environment, real-life dangerous situations are rare. However, our physiology isn't able to draw a distinction between news of horrible events or dangerous situations, and the actual experience of personally experiencing one.[231] Adults (but not young children) are able to consciously counter negative emotional reactions with rationalizations and context; we can watch a horror movie and tell

[230] *https://www.theatlantic.com/newsletters/archive/2023/03/negativity-bias-online-news-consumption/673499/*
[231] *https://www.nature.com/articles/s41562-023-01538-4*

ourselves "these are just actors, this is just a movie, it isn't real, I'm not in danger." Furthermore, being safely abstracted from a horrible situation actually makes us feel good; something bad happened to someone else, but we ended up safe in the end.[232] With this in mind, you can see why it's so important for advertising and propaganda to manipulate our senses. But at what cost?

I've already cited some research and leaked internal memos that reveal how social media consumption negatively impacts mental health, and there are dozens more I could list here. Currently there isn't as much research on how consuming negatively-biased traditional media and data-driven ads directly impacts consumers, but since social media is largely composed of algorithmically-curated links to traditional media and personally-targeted ads, we can reasonably infer that they are at least partly (probably mostly) to blame. I do have one case study to cite in the next section, but before you read that, I want you to ask yourself these questions:

- How many times can I be angry, shocked, offended, or disgusted before my mood is ruined for the rest of the day?
- How does my behavior – especially my consumption habits – change when I'm repeatedly exposed to these emotional states?
- How can I stay reasonably informed about current events without sacrificing my emotional well-being and physical health?

Development of Addictions and Compulsive Behaviors

Arguably the most insidious form of data-driven manipulation of ordinary people is by using consumer products and services to develop, refine, and monetize addictions and compulsive behaviors in them. Even worse: children are often the preferred target.

From a medical standpoint *addiction* is a complicated topic. It used to refer solely to the physiology of chemical dependency, whereupon someone regularly ingests increasingly larger amounts of a psychoactive substance over a long enough period of time to the point that his or her body adjusts

[232] *https://www.verywellhealth.com/what-happens-when-you-watch-horror-film-8365111*

to its presence; when the supply of that chemical is cut, the body reacts as though something critical is missing (withdrawal). More recently, *addiction* evolved to encompass the pathology of people who are highly susceptible to drug use and chemical dependency. Today, the American Psychiatric Association has begun to separate "substance abuse disorders" from non-substance-based "addictive disorders," and the World Health Organization includes several addictive pathologies under the Obsessive-Compulsive and Related Disorders category in its International Classifications of Disease, 11th Edition (ICD-11). Such pathologies are broadly defined as:

> *The repeated failure to resist an impulse, drive, or urge to perform an act that is rewarding to the person (at least in the short-term), despite longer term harm either to the individual or to others.*

As of this writing, the psychiatric community is still considering how to define and categorize various types of addiction-like behaviors that are commonly found in modern patients.[233] Probably because it's been around for a long time and has a lot of clinical evidence behind it, compulsive gambling is the most solidly-defined among "behavioral addictions," but there are several other behavioral disorders that share many of the same psychological and biological phenomena and treatments as substance-based addiction, and there is a high degree of co-occurrence between substance addictions and non-substance-based compulsive behaviors such as:

- **Sex addiction**: hypersexuality or nymphomania
- **Internet addiction**: excessive Internet or social media use
- **Gaming addiction**: excessive participation in online games
- **Kleptomania**: compulsive stealing
- **Shopping addiction**: compulsive shopping or "retail therapy"
- **Junk food addiction**: compulsive overeating or binge eating

[233] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5328289/*

- **Pyromania**: obsessive starting of fires
- **Intermittent Explosive Disorder:** compulsive violence

Ultimately it doesn't matter whether these problems are classified as "addictions" or "obsessive behaviors," or whether they are on the same level as drug or alcohol addictions; what matters is that they will all eventually destroy people's lives, and that one seemingly harmless addictive behavior can easily lead to others – including drug and alcohol abuse – and that addictions and compulsive behaviors often lead to criminal activity.[234] For instance there are many well-documented cases of compulsive online video-gamers who have committed suicide, or violently attacked or murdered their parents or fellow gamers as a direct result of their video game addiction.

All addictive behaviors begin with repetitive actions and pleasurable rewards. Over time, the rewards become more difficult to earn, or require an increasingly larger investment of time or money. The social media and **massively-multiplayer online** (**MMO**) game industries survive and profit by their ability to drive engagement. For instance on X, *engagement* means tweeting, retweeting, following, and Liking; the service is designed to make users feel like there's always something new to see and interact with in their feed, and if you aren't getting enough attention, then you can pay to promote your account or your content. In an MMO game like *Final Fantasy 14* or *World of Warcraft, engagement* means leveling your character by completing quests, gathering materials, crafting in-game items, killing monsters, and forming groups with other players to clear a dungeon or large-scale raid – all of which grants the player various rewards. MMOs employ digital dark patterns to make users feel like there's always something to do to build or improve their status in the game world. Just like with social media, MMOs and other multiplayer games sell shortcuts to virtual status via exclusive cosmetics or "skins," level boosts, and powerful in-game items that make it easier to win or advance.

In other words: social media apps and MMO games are designed to be addictive (to encourage excessive use and generate compulsive behaviors), and the more information their developers have about their users, the more effective they are at getting people hooked on their services. Nearly every American knows at least one person who is obviously addicted (in

[234] *https://pubmed.ncbi.nlm.nih.gov/27192094/*

the colloquial – not clinical – sense) to social media, either by **oversharing** (revealing extraneous personal information with the hope that it will generate more engagement), constantly posting content, or **doomscrolling** (compulsively refreshing the content feed to see new things). Seldom do any such "addicts" appear to be – or will even claim to be – having fun or experiencing joy; in fact they seem to be miserable much of the time, which credible research on the topic confirms.[235] YouTube is full of unfortunate examples of compulsive online gamers who fly into a violent rage when they do not earn the expected rewards for the time and money they've invested in a video game. When addicted gamers feel that other players have caused them to lose or to delay progress, they often become extremely abusive toward them or retaliate by sabotaging their gameplay – behavior that the game service provider will punish them for despite the fact that the game was engineered to foster the addiction that leads to this kind of reaction in players.

Perhaps the worst aspect of addictive online services is **re-engagement** efforts, where the company sends personally-targeted "come back to us" incentives to you and your online connections to try to pull you back in. Such tactics can include: fee waivers, "free" digital goods such as in-game items or add-ons, virtual currency bonuses, temporary higher visibility of new content that you post, and teasers of high-engagement content posted by your friends and family. The point is not just to get you re-engaged with the service, but to create **the fear of missing out (FOMO).**

Dealing with addictive behaviors is very difficult to handle on your own. If you suspect that you might be addicted to a game, social media service, or sports gambling app, you owe it to your family and community to seek professional help as soon as possible. There are a variety of different treatment options to accommodate a variety of different cultures, religions, and other circumstances, and most of them are effective in helping people overcome addiction and addictive or compulsive behaviors. In addition to searching for therapists and support groups in your locale, here are a few others to consider:

- **GameQuitters**: https://gamequitters.com

[235] *https://www.scientificamerican.com/article/why-social-media-makes-people-unhappy-and-simple-ways-to-fix-it/*

- **Online Gamers Anonymous**: https://www.olganon.org
- **It's Time to Log Off**: https://www.itstimetologoff.com
- **The National Council on Problem Gambling**: https://www.ncpgambling.org or 1-800-GAMBLER

In addition to the advice I've already given, here are some things you can do to prevent corporations from sucking you into their vortex of addiction:

- Even if you're certain you're not addicted to anything, take a moment to ask yourself these questions:
    - What do I most often do when I feel like I need to escape from negative feelings, trauma, or stress?
    - How would I know if I had an addiction or gambling problem?
    - How much money are service providers making from my participation, subscription, cash purchases, and/or engagement?
    - What might those companies know about me based on my participation and billing information, and how could they use that data to convince me to give them more of my time and money?
    - Am I actively having fun doing this, or am I actually kind of bored, but feel like I should "grind" or "doomscroll" to chase the small and short-lived pleasure of occasional participation rewards?
    - What would my life be like if all games and social media services shut down forever? How would I spend my time differently? How would I connect to friends and family? Where would I go to read or watch the news?
- Block and mark as "spam" any re-engagement offers you get from games and apps that you no longer wish to use, and ask your friends and family not to participate in them on your behalf.

Online Gambling

Think back to the card game example from earlier in this chapter, where an opponent offers to pay you $5 to play with all your cards facing up. As a metaphor for trading your valuable personal information for a lesser- or negative-value prize, it works. But taken literally it's an unrealistic scenario for online poker games and sports gambling apps because I specifically gave you the extreme disadvantage of having your cards always laid face-up on the table. It isn't far from the actual reality of the marketing practices of online gambling services, though. The bedrock promotional strategy for gambling platforms is a discount or credit for your first bet. If you only ever make one affordable bet, this isn't really a problem. Neither is just smoking just one cigarette.

Another angle you could take on the card game scenario is that you paid $15 to have a fun evening playing cards. You could've spent more than that on a mediocre Marvel franchise movie, or a pay-per-view boxing match that ends in the first round. Beware; this is a slippery slope. Gambling is a form of entertainment, but – like tobacco or recreational drug use – it's also a well-documented addictive behavior that can quickly get out of control and ruin your life, and once a gambling company gets hold of your personal information, your chances of "just one bet" turning into tens of thousands of dollars of debt increase substantially.

Though casinos are illegal in most of the US, the legalized casino industry in America (and on tribal land) generated $329 billion in revenue in 2022.[236] While about $52 billion of that was paid out in Federal tax, and $100 billion was paid out in wages, in general this money generated no useful production in the US economy. In other words, people gambled away $329 billion that they could have spent on home improvements, vehicles, home electronics, dining out, school tuition, or family vacations. It also likely was a major factor in accruing high-interest debt.

When playing against **the house** (the casino or gaming operator), the odds of winning are heavily stacked against the player because every game's rules are designed to favor the house (**the house edge**). Professional gamblers do exist, but they largely make their money playing against other people (in poker, usually) where the odds favor the most skilled players. Even in

[236] *https://www.usnews.com/news/us/articles/2023-10-09/casino-industry-spurs-329-billion-in-us-economic-activity-study-by-gambling-group-shows*

poker, though, the house takes a cut from the winning pot (**the rake**), so the house always makes money no matter who wins the hand.

Traditional casinos are masters of maximizing profits. Before the era of modern technology, casino managers collected personal data the hard way and used it to their advantage by quickly identifying **high rollers** (wealthy people who spend a lot of money) and offering them **comps** (gifts given to certain customers at the discretion of management) in the form of free hotel rooms, food, alcoholic drinks, tickets to shows, luxury transportation, and sometimes expensive goods like designer clothing and new cars.[237] You don't even need to be a high roller to get some low-level comps; in most casinos, merely sitting at a gaming table with a stack of chips will net you a series of free drinks. When someone **beats the house** (defies the odds and wins a lot of money), regardless of whether it's through pure luck, cheating, or a good memory and clever reasoning (**card counting**), they're immediately detected and prohibited from playing at certain gaming tables, escorted out, or banned from the casino, despite laws designed to protect "skilled gamblers."[238] In the old days this was done by using a small army of highly-trained observers; today it's done at least partially through technological means.

In the past you had to go to a casino to legally gamble (or to a mafia bookie or backroom poker game to do it illegally), and this was a significant limiting factor for people who suffered from gambling addictions. Now that online gambling is largely legalized (and poorly regulated) in the US, those people can play online casino games or make sports bets from their mobile devices and computers without leaving the house – and without detection from their family members.[239]

Online gambling – in the form of virtual poker tournaments and casino games, and legal (as of the publication of this book) professional sports betting apps such as DraftKings and FanDuel – are much more accessible, and therefore dangerous for people who suffer from gambling addictions. What passes for "normal" personal information collection and targeted marketing with most online services may, with online gambling, cross the

---

237 https://www.casinolifemagazine.com/blog/revealed-perks-casinos-offer-keep-high-rollers-playing
238 https://apnews.com/general-news-fdd01bfe9d0b438685f4a72e03a067f5
239 https://www.ft.com/content/23208913-7ff4-4772-a329-33ec5cc2392a

line between "driving engagement" and "encouraging problem gamblers to relapse."[240]

Beyond personal targeting, gambling apps constantly pester users to spend more money via **proposition bets** (side-bets on particular aspects of a game, such as betting that a certain player scores a minimum number of points) or **parlays** (when proposition bets or similar specific criteria are made into conditions of the main win/lose bet, making the main bet less likely to pay out). By buying into those options, a gambler can end up feeling good that his team won the game even though he lost money on the conditional bet. Remember: gambling apps make the most money when you lose, not when you win, so they're incentivized to push you into losing by raising the stakes.[241]

If you have ever felt remorse for losing too much money to a bet or game, or if you've ever felt euphoric after beating the odds and winning money, I implore you to stay away from all forms of online gambling. It's relatively easy to refuse to go out to a real casino or off-track betting parlor, but all you need to do to re-engage with a gambling or casino gaming app is click a link in an email designed specifically to appeal to your interests and insecurities.

If you're at all concerned about getting involved with the financial death-spiral of online gambling, here are some actions to take:

- Never install a gambling app on your mobile devices.
- If you get a marketing email from a gambling service, mark it as "spam" and consider setting up a rule in your email client or service to block all communications from that email address. Don't even try to use the "unsubscribe" or "opt-out" links in these emails – they lead to landing pages that may offer personally-targeted incentives.

240

https://web.archive.org/web/20210324150717/https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking-sky-bet.html

241 https://fortune.com/2023/02/06/how-sports-gambling-betting-apps-work-addictive-psychologist/

- Consider some alternative ways you can exercise your competitive spirit without making bets. In the right circumstances, the glory of winning and agony of defeat don't need to be amplified with cash.

Obsessive Video Gaming

> *There are some aspects of this business model that make it so – you're not making games to be fun anymore. You're playing to – here's the stuff that addicts players, that makes people come back. You're implementing these strategies to hook people, but they're not necessarily having fun with your game anymore. They're compelled to play because they need to increase their level or feel like they're making some other kind of progression. But if you asked them, "Hey, take a step back. Strip away all of this. Is the moment to moment gameplay fun for you?" in a lot of cases I bet the answer would be 'no.'*
>
> *-George Fan, designer of the Plants vs. Zombies game*[242]

Playing video games can be a fun hobby, but when more important aspects of your life are going wrong (doing poorly in school, being unemployed, going through a divorce, having a close family member with a medical crisis or terminal illness), it's easy to dissociate from the stress by escaping into an addictive game – and all addictive games have multiple methods of extracting as much time (engagement) and money from players as possible. Stories abound on the Internet of people who have sacrificed their education, career, and marriage for online games, most notably *World of Warcraft*.

Playing video games becomes a problem when it encroaches on time that a healthy person would spend on school, a career, their family, and social time with real-life friends in real-world places. Cam Adair, a former video

[242] *https://venturebeat.com/business/how-george-fan-created-the-wacky-plants-vs-zombies-a-decade-ago/view-all/*

game addict and current founder of GameQuitters (`www.gamequitters.com`), lists these four components of addictive video games:

1. **Temporary escape** from stressful life situations with one's health, work, school, romantic and social relationships, and mental health issues such as depression and anxiety.

2. **Social connection** to other people in gaming communities that share similar circumstances and also seek to escape the stressors of the outside world. An online gaming community can feel like a "safe space" for addicted gamers, and provide a virtual social environment to replace physical social spaces that may cause anxiety or feel exclusionary due to mental illness or lack of local connections.

3. **Constant measurable growth** through game frameworks that record progress in terms of points, achievements, and statistics.

4. **A clearly-defined sense of purpose** through game systems that provide a concrete quest, mission, or task, and criteria for success. Addictive games always have clearly-defined next steps that players can work toward, and rewards in the form of in-game items, badges, and virtual currency.

None of the items in this list are, in themselves, harmful or even abnormal behaviors. As social animals, humans need to occasionally step back from trauma or overwhelming stress in order to figure out how to cope, and social connection to like-minded peers is essential to our emotional well-being. Constant measurable growth and a clearly-defined sense of purpose are key aspects of learning any skill. One cannot learn to play the guitar, for instance, without experiencing the "dopamine hit" rewards of measuring your progress and achieving realistic goals (such as learning how to play a difficult guitar solo, or your favorite song). It's critical for gamers to recognize the difference between building useful skills and "grinding" through repetitive video game content to obtain rewards.

The details of how we handle item 1 (temporary escape) are critical to whether we go on to focus our energy in a healthy way. If someone chooses self-destructive methods of escape instead of actively working toward discovering and cultivating constructive coping methods, then everything in the list after that will be tainted by that choice, and open the

door to addiction. Social connections turn into enablers, and measurable growth and a sense of purpose become lies and delusions that feed back into the desire to escape.

When a gaming company gets hold of your personal information – especially your willingness to purchase add-ons, expansions, loot boxes, and cosmetics – it will develop ways to extract more money from you with special deals, customized offers, and in-game bonuses to keep you hooked on the service when your attention and purchases start to wane. If you quit the service, then you can count on the company going to great lengths to pull you back in via discounts and "free" items delivered to you by email, mobile notifications, social media, and special offers for your in-game friends if they pester you to rejoin. Game companies zealously employ various digital dark patterns to drive engagement and monetization.

To their credit (or rather as a result of the fear of government regulation and private litigation), most online gaming companies offer extensive parental controls features to enable parents to put hard limits on how much time and money their kids can spend in a game, and how they can interact with other players. If your kids play online games, you must commit to monitoring and limiting them through parental controls. If you don't have kids, parental controls are also helpful for forcing yourself to stick to the limits you're comfortable with. It's easy to tell yourself ahead of time that you'll spend no more than 6 hours per week or $15 per month playing a game, but it's even easier to blow past those limits when the game isn't programmed to force you to curb your impulses.

Political Manipulation and Civil Unrest

> *The propagandist's purpose is to make one set of people forget that certain other sets of people are human.*
>
> *-Aldous Huxley*

We are changed by what we consume, both physically and socially. When we consume factual information, we expand our minds by becoming more informed about the world; when we consume lies and propaganda, our perspective narrows and we become not only ignorant of objective reality, but also dependent on liars and propagandists to supply us with

increasingly stimulating and provocative content. Consuming information from an unknown or untrustworthy source is no less risky than consuming food or drink without knowing who prepared it or what the ingredients are. If some random guy or gal on the street were to give you a mystery liquid and asked you to drink it, hopefully you wouldn't agree; neither should you accept any new information from random YouTubers, fringe websites, or social media accounts. Unfortunately people you know and trust may sometimes try to pull you into the quagmire of conspiracy theories and political propaganda, believing that they are helping you to see the invisible "truth" hidden in a web of lies and fantasies. Even the most honorable, intelligent, worldly, and educated people are susceptible to cleverly-crafted propaganda and influence campaigns, and personal data-driven algorithms are largely to blame.

As I explained in Chapter 3, real-world espionage is mostly a matter of collecting and selectively releasing (or threatening to release) personal, private, and secret information; it is extortion at the highest level.[243] Unless you are a politician, member of the military, or are otherwise required to maintain a Secret or Top Secret clearance with the US Department of Defense, you probably don't have to be concerned with foreign agents trying to manipulate you into becoming a spy. That doesn't mean that foreign governments aren't out to get you – it just means that for most people the flow of information is reversed.

The other side of the espionage coin is **disinformation** (specially-crafted lies that are published and propagated with the intention of manipulating a certain group of people to behave in a disruptive or self-destructive way). Sometimes disinformation creates behaviors that are directed inward, such as to hide immoral government activities or mistakes from its citizens, or to influence the outcome of elections. More commonly, though, it's directed outward at the citizens of rival nations: foreign agents seeking to disrupt their enemies by causing civil unrest.[244]

Disinformation takes the following forms:

---

243 https://www.gq.com/story/cia-investigation-and-russian-microwave-attacks

244 https://web.archive.org/web/20220507153720/https://www.wired.com/story/putin-collapse-disinformation-machinery-ukraine/

- **Fake news**: articles and "deepfake" photos and videos that portray, describe, or depict an event that has not occurred. Sometimes this takes the form of a legitimate video or photo from one event (such as a battlefield in Afghanistan) that is purported to be from a different event (such as a scene from the war in Gaza).

- **Manufactured rumors**: social media posts and comments (usually from fake, or anonymous or pseudonymous accounts) that seek to create fear, uncertainty, and doubt about certain political and social topics with the hope of derailing honest public discourse and encouraging people to seek out "alternative" (fake) news sources.

- **Fake science**: academic papers transparently designed to support a political agenda, published in journals that do not have an adequate peer review process. Such papers are not merely sloppy or flawed (as is the case with "junk science," explained later in this section); they are based on nonexistent research or fabricated data.

- **Big lies**: when politicians and other public figures knowingly and willfully publish, utter, or broadcast false messages to support their personal goals. When those false messages are relentlessly reinforced by famous and/or powerful people in popular media and large public venues, big lies can be effective despite the fact that they can be quickly and easily disproven through a variety of credible sources.

Another weapon used by both foreign agents and domestic propagandists of various kinds is **misinformation**, which is media that uses partial truths or discredited sources to establish and reinforce a false belief. Whereas disinformation is an outright falsehood, misinformation is crafted similarly to factual information: it cites sources (though the sources are either unreliable or have been discredited by reliable sources or proven to be untrue, such as scientific studies that failed to pass peer review, or court cases that have been overturned on appeal), and quotes subject matter experts (though they aren't actually credible experts on the topic; often these quotes are from celebrities, social media influencers, self-appointed gurus, or experts on topics other than the one being covered; for instance a podiatrist commenting on the technical capabilities of a commercial airplane). Sometimes even credentialed experts are motivated by self-interest or political pressure to create and amplify misinformation.

The most common forms of misinformation are:

- **Clickbait**: provocative media that disrupts a truthful narrative through misleading headlines; sometimes the article or video itself presents credible facts even though the headline questions, distorts (through exaggeration or hyperbole), or disputes them.

- **Conspiracy theories**: a small set of verifiable facts and truths connected by a false, self-destructive narrative created to disrupt political and social institutions. As conspiracy theories grow and evolve, they typically incorporate disinformation into the narrative.

- **Hate speech**: media or social media content that openly blames society's ills on a specific sex, sexual orientation; or political, ethnic, or religious group, usually by way of citing other sources of misinformation and disinformation.

- **Junk science**: similar to fake science, except junk science is based on unproven belief systems such as metaphysics, biased and improperly-conducted opinion polls, or old theories and studies that were genuinely believed to be true at one time, but have since been thoroughly discredited, retracted, or disproven through credible research, replication, and peer review.

Misinformation is always interconnected by way of the Internet and political punditry. Junk science and clickbait articles feed conspiracy theories, and all conspiracy theories eventually converge and lead to hate speech (most commonly of the antisemitic variety). The algorithms that drive engagement on social media (especially video services like TikTok and YouTube) and search engines (aside from the privacy-focused options I covered in Chapter 2) use the data you give them to show you increasingly provocative content that quickly leads down a rabbit hole of misinformation and disinformation with the hope that you'll click on some ads along the way.[245]

Political commentary on television and radio is an incubator, launchpad, and amplifier for misinformation and occasionally disinformation as well; this is because it survives on rage-farming:

---

[245] https://www.theatlantic.com/technology/archive/2023/08/youtube-rabbit-holes-american-politics/675186/

> *We have people who -- on the radio and TV, and we all could go down the list of people -- who are there for one reason only, and that's to make you mad. And the formula for making you -- the viewer or the listener -- mad hasn't changed a bit, yet people keep falling for it. It amazes me.*
>
> *-Rush Limbaugh*[246]

Sometimes misinformation and disinformation are merely tools for generating ad clicks and radio and television ratings – a perverse form of popular entertainment on "free" platforms and networks – but increasingly they are used as weapons in the information wars among political parties and between democratic nations and autocratic regimes (largely Russia, China, and India). Engagement algorithms powered by personal data are quick to deliver provocative search results and content recommendations that contain messaging designed to undermine democracy and destroy Western social institutions. According to the US Department of State, the Russian government in particular is heavily invested in weapons of mass deception:

> *Disinformation is one of the Kremlin's most important and far-reaching weapons. Russia has operationalized the concept of perpetual adversarial competition in the information environment by encouraging the development of a disinformation and propaganda ecosystem. This ecosystem creates and spreads false narratives to strategically advance the Kremlin's policy goals. There is no subject off-limits to this firehose of falsehoods. Everything from human rights and environmental policy to assassinations and civilian-killing bombing campaigns are fair targets in Russia's malign playbook.*

[246] *https://www.youtube.com/watch?v=FH0QhvnPTP0*

> *Truth disarms Russia's disinformation weapons. The Kremlin creates and spreads disinformation in an attempt to confuse and overwhelm people about Russia's real actions in Ukraine, Georgia, and elsewhere in Europe. Because the truth is not in the Kremlin's favor, Russia's intelligence services create, task, and influence websites that pretend to be news outlets to spread lies and sow discord. Disinformation is a quick and fairly cheap way to destabilize societies and set the stage for potential military action. Despite having been exposed for engaging in these malign activities countless times, Russia continues to work counter to international norms and global stability.*[247]

In addition to fake news stories and big lies, the Russian government also pays for entire office buildings full of people (in Russia, Macedonia, Kosovo, and elsewhere) to create fake social media accounts (using profile photos and other details copied from legitimate social media users) and pages, and use them to post content and comments on platforms such as Facebook, X, Reddit, and in the comment areas of legitimate news sites. Facebook is particularly valuable to disinformation agents; Russian trolls reach as many as 140 million Americans per month through that platform alone (for reference, Wal-Mart's reach on Facebook is about 100 million).[248] Pages and posts largely focus on creating social discord by inflaming racial, gender, and religious issues. At one point in recent history, Russian trolls controlled the largest Christian American and African-American Facebook pages, and among the largest pages for Native Americans and women. And in 2018, the US Federal Trade Commission fined Facebook $5 billion for selling personal data on 87 million users to a third-party company (Cambridge Analytica), which then used it to spread

[247] *https://www.state.gov/disarming-disinformation/*
[248] *https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/*

micro-targeted misinformation and disinformation on behalf of politicians and organizations with ties to Russia.[249][250]

I could write an entire book full of case studies about the algorithmic spread of misinformation and disinformation, but I've narrowed it down to the few that I feel are most representative of personal information exploitation. Before I present them to you, I'd like to clarify that the spread of propaganda, disinformation, and misinformation is a direct result of media and technology companies collecting and using your personal data. By that I don't just mean your name, age, and other superficial details; I also mean less tangible things like the links and ads you click on, your app usage habits, your purchase history, the accounts that you Follow or Like, and the topical interests that you unconsciously express simply by using Facebook, X, Instagram, Google, TikTok, YouTube, and other similar services.

At times it may seem that I'm focused largely on the evils of social media, but that's strictly because social media services use engagement algorithms that attempt to target every individual user with content and ads that they are likely to be interested in (or enraged by) regardless of whether they make life better or worse for them (and it's almost always worse). Personal data is the lifeblood of social media – it's what makes their owners and executives wealthy – and social media platforms are the central nervous system of propaganda, misinformation, and disinformation campaigns. Without the ability to "go viral" on social media, disinformation would largely fall flat.

I'm also worried that social media companies may not be honest when they claim that their recommendation algorithms are intended to introduce users to content that they are likely to be interested in. At very least, I'm sure that's not the whole story. It is very easy for those companies to alter their algorithms to show you what the company executives or advertisers want you to see, and to demote or erase any pages, posts, photos, videos, or other content that is either unprofitable or contains disfavored viewpoints or contrary evidence. According to reporting from *The Verge,* I already know for a fact that Elon Musk ordered his engineering team to

---

[249] *https://www.straitstimes.com/world/united-states/cambridge-analytica-shared-data-with-russia-whistleblower*

[250] *https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal*

make his tweets more visible to people on X, and I'm gravely concerned that this one documented act of narcissism is just the visible tip of the altered-algorithm iceberg.[251]

Case Study: 2014: The Year of the Russian Hoax

Internet hoaxes are almost as old as the Internet itself, but up until the 2010s hoaxes were largely small-time pranks or scams that unexpectedly became popular. If I were to identify two points in history that were most impactful to the power of personal data, they would be 2008 when Barack Obama's presidential campaign employed data scientists to successfully maximize online donations, and 2014 when the Russian government went all-in on organized online disinformation efforts.

It's difficult to put Russia's anti-Western propaganda on social media into perspective because it is thoroughly integrated with legitimate political and social concerns, most notably racism against American black people. At the highest level, political propaganda is most effective when it targets contemporary concerns, fears, and desires. This is why sharing your personal information with social media companies is so dangerous; by identifying with a cause, community, or demographic, you paint a target on yourself for social media companies' engagement algorithms (to show you things that upset you) and for their advertising clients, which include corporate marketers and political propagandists.

Over a period of several months in the latter half of 2014, Russian agents at the notorious St. Petersburg-based Internet Research Agency waged a full-scale information war to destabilize American society in general and Western social media in specific by weaponizing social media in an attempt to cause widespread panic and civil unrest.[252] The three most widely-reported examples are in the subsections below.

The Columbian Chemicals Plant Explosion

On September 11, 2014, someone posted a video to YouTube apparently showing a fiery explosion at the Birla Carbon Columbian Chemicals Plant

[251] *https://www.theverge.com/2023/2/14/23600358/elon-musk-tweets-algorithm-changes-twitter*
[252] *https://www.nytimes.com/2015/06/07/magazine/the-agency.html*

in Centerville, Louisiana.[253] Shortly after, residents of the area surrounding the plant were sent SMS text messages from an unknown number claiming: "Toxic fume hazard warning in this area until 1:30 PM. Take Shelter. Check Local Media and columbiachemical.com." On Twitter (X), hundreds of eyewitness accounts of the incident sprang up with the hashtag #ColumbianChemicals, along with screen shots of and links to what looked like credible news coverage of the story. Another YouTube video was posted in which the terrorist group ISIS allegedly claimed responsibility for the attack.

Credible news agencies didn't actually report on the explosion, though, because it never happened; a simple phone call or visit to the plant quickly and easily confirmed that no accident or incident of any kind had taken place there or anywhere else. Rather it was the result of perhaps the largest, most expensive, and highly-coordinated public disinformation campaign in history, and it was mildly and temporarily successful in creating panic not just in Louisiana, but across the entire country.

The video was fake, as was the text message and the website it pointed to for more information. The fake news stories were not just on "alternative" news sites; they were on sites that were exact clones of legitimate local newspapers and TV stations, and social media posts included fake screenshots from larger reputable sources such as CNN and the New Orleans Times-Picayune (which did not actually publish the stories shown in the images). The social media posts were not just spammed willy-nilly to the Twitter masses, they were designed to draw the attention of specific influencers and public figures. There was even a fake Wikipedia page documenting the explosion and citing fake news and social media posts as sources.

In the ensuing months, FBI analysts and independent investigators determined that the Columbian Chemicals Plant explosion hoax was perpetrated by the Internet Research Agency in St. Petersburg, Russia.[254]

---

[253] https://en.wikipedia.org/wiki/Columbian_Chemicals_Plant_explosion_hoax
[254] https://www.npr.org/2024/03/14/1238514552/how-to-win-an-information-war-details-fighting-with-and-against-propaganda

Ebola Outbreak in Atlanta

In the wake of a handful of legitimate (but contained) Ebola infections in the US, on December 13, 2014, Russian agents took another shot at using social media and fake news to cause panic and disorder in the US by claiming – through the same means (and even the same fake social media accounts) as the Columbian Chemicals Plant hoax – that there was a massive outbreak of Ebola in Atlanta, Georgia. Fake videos and images, cloned websites, and false eyewitness accounts flooded Twitter with the hashtag #EbolaInAtlanta.

Again this disinformation attack was briefly and mildly successful in creating public anxiety, though it was much more quickly discredited and defused because the Internet Research Agency's playbook had already been exposed three months prior in the Columbia Chemicals plant hoax.

Police Shooting of a Black Woman in Atlanta

It's a well-documented fact that on August 9, 2014, 18-year-old Michael Brown was shot and killed by police in Ferguson, Missouri. This proved to be a tipping point for several long-simmering issues in American society: the militarization of police agencies, the overzealous and often selective enforcement (discriminating against black people) of minor crimes, and a highly-publicized history of police using excessive violent (often lethal) force against impoverished suspects. Protests and riots erupted in Ferguson and elsewhere, and every branch of the local, state, and Federal government became involved with containing the fallout and developing ways to make the justice system less violent and more equitable.

For Russian disinformation agents, Michael Brown's death was the perfect opportunity to make things worse for Americans, much like the reports of a few isolated Ebola cases in the previous case study.[255] In fact the Internet Research Agency even pulled double-duty to create and attempt to publicize (with the hashtag #shockingmurderinatlanta) a fake news story about Atlanta police killing a black woman on the same day as the fake Ebola outbreak. Both disinformation campaigns cited fake videos, fake news stories, and fake eyewitness accounts on social media; the main

[255] *https://en.wikipedia.org/wiki/Russia_and_Black_Lives_Matter*

difference between them was that this one used a different set of fake social media accounts.[256]

256

https://web.archive.org/web/20240124033557/https://www.nytimes.com/2018/08/14/technology/facebook-disinformation-black-elevation.html

Chapter 6: Opting-Out and Locking Down

No matter what you do right now and in the future, your digital privacy has already been permanently compromised through multiple corporate data breaches and clandestine collection and mass-resale by data brokers. There's hope, though; some personal information becomes irrelevant over time (if you change your home or mailing address, phone number, email address, name, etc.), and with a little effort, you can undo some of the damage – and keep it from getting worse in the future – by **opting-out** (preventing your information from being shared), **locking down** (preventing your information from being collected), and **under-sharing** (limiting what you share publicly and with corporations).

Before I go into specific topics, here are a few general tips for increasing your privacy and security right now and in the future:

- Reduce the volume of phone spam by adding your phone number(s) to the US Federal Trade Commission's Do Not Call registry: https://www.donotcall.gov/. This won't stop scammers, but it will stop companies from calling you if they've harvested or legally purchased your personal information.

- If you move to a different residence, be sure to file for a change of address with the US Postal Service (but don't opt-in to any "special offers" or "free" coupons in the process), and spend some time thinking hard about every bank, credit card company, utility, subscription service, and any other important financial relationship, then update your accounts with your new home address (using your PO box or mail receiving service as your official mailing address whenever possible). You don't want any mail to end up at old addresses. Even junk mail can reveal some of your personal information to unintended recipients.

- Avoid signing up for or participating in anything that requires giving up your home address, phone number, or email address unless it's important. That means no contests, giveaways, polls, raffles, discount and rewards programs, opinion surveys, mailing lists (duh!), "free" things, and unnecessary user accounts for apps and websites. If you choose to participate, use a masked email address and your PO box.

- Never publish your email address, home address, or phone number online. Spammers and scammers constantly **scrape** (use a script to copy the content and layout of a webpage) this information from websites.

- When possible, do not consent to information sharing via cookies when prompted by a website.

Go Back to Paper Billing

In the 1990s and early 2000s mail theft and dumpster-diving were the most common vectors for identity theft. Consequently every business, service provider, and utility company recommended switching to email-based (or "paperless") billing, not only as a security precaution, but also to save them the cost of printing and mailing your monthly bills and statements. While those methods of information collection are still a concern, in the modern world you're much more likely to fall victim to email phishing schemes than paper mail theft. Modern thieves know that a lot of people use paperless billing, and it's easy for them to guess which utility companies and other service providers you use, then send a phishing email pretending to be your water authority or mobile service company. If you follow my

advice religiously, then those emails shouldn't be effective, but as I showed you in Chapter 2, timing is everything. If you're expecting your Verizon bill on the 15th of each month, and a Verizon-based phishing email gets to your inbox on that day ahead of the real e-bill, then you might not give it the scrutiny it deserves. E-billing is also increasingly being outsourced to third-party companies, so you might become accustomed to your legitimate bills being sent by strange email addresses and including links to strange URLs.

Earlier in this book I said that paperless billing is a good way to prevent identity theft via dumpster-diving. That's true, but increasingly it may present more risk than it mitigates, depending on the context. Dumpster-diving is negated by shredding (or otherwise destroying) your discarded mail and documents, and receiving all of your mail at a PO box removes the possibility of mail theft (dishonest postal workers and misdeliveries aside). Under these conditions, your personal information is safer if you switch to paper billing.

Reduce Your Information Footprint

When you walk on unpaved land, your movement creates footprints that reveal your approximate size and the details of where and when you traveled. Similarly when you do anything online, you leave a trail of digital footprints; unlike its physical counterpart, though, an information footprint can be easily recorded, profiled, and shared. Following my advice in Chapters 1 and 2 will effectively obscure your footprints in most situations, but ultimately the best policy is to leave as few footprints as possible.

When a corporation has collected your data, it tends to want to keep it forever, even if it ends up costing them time, money, and reputation in the future by way of a data breach. Assume that every company and government agency that collects and stores your personal information will suffer one or more data breaches in the future. In many instances you have the right to ask companies to delete the data they've collected about you, or at very least to provide you with a copy of it (though I'm not sure how that's helpful). Frustratingly, as I explained in the Blackbaud case study in Chapter 3, they don't always follow through on their promise to delete customer data. That doesn't mean you shouldn't try.

Sometimes you have the legal right to request that future information not be collected or shared, and to opt-out of marketing communications (which are augmented by your personal information), but you'll have to read the fine print carefully to figure out how to do this and what the time limitations are. Capital One, for instance, offers new customers a grace period of 30 days to opt-out of its information-sharing practices, but you have to call a special phone number and request it before the deadline.[257]

Various methods for obscuring or removing your digital footprints are in the subsections below.

Avoid Creating New Accounts

Every time you buy something from a website, you're asked to create an account with that merchant to record your personal information, ostensibly to make it easier to buy more stuff in the future. If you don't save your email invoices and receipts, then creating an account can also help you view past orders and track current ones. Many merchant sites don't have top-grade information security, though, and eventually will suffer a data breach, or someday they will be sold to other companies that may use your information in unanticipated ways. While your credit card details aren't critical – you can easily reverse any fraudulent charges made to a credit card – your personal information can repeatedly be used against you by scammers and spammers. Even worse, many online merchants use PayPal for payment processing and order management; I could write a whole book on the awfulness of PayPal – avoid it whenever possible.

You can almost always make a purchase as a "guest" without creating an account or storing any information with an online merchant or payment processor. Your email address and shipping address will probably still be added to marketing lists, but this is less of an information footprint than creating a user account, and you can opt-out of the mailing lists.

If you already have an Amazon account, then there isn't much further harm in using it with merchants that rely on Amazon for payments and order fulfillment. Ideally you wouldn't have an Amazon account either, but the current reality of e-commerce makes avoiding Amazon a near impossibility.

---

[257] *https://www.capitalone.com/privacy/notice/*

Opting-Out of ISP Information Sharing

Internet service providers are the biggest collectors of digital footprints. They are in charge of assigning you an IP address, and they often provide the modem and wireless router for customers as well, so they have the MAC address of your network hardware and every device that connects to it. They also log your exact path to every site and service you use on the Internet, and keep a record of the media you access and the files you download. Using a VPN negates much of this information collection for home Internet services, but it can't block cellular service providers from recording SMS / MMS text and voice data (what ISPs refer to as **customer proprietary network information**, or **CPNI**).

You cannot prevent CPNI from being collected, but you can instruct Internet service providers (both home and cellular) to refrain from using and sharing it for marketing purposes. You can use a search engine to find the opt-out procedure for your providers. Here are the opt-out URLs for the three largest companies:

- **AT&T**: `https://www.att.com/ecpnioptout/InitiateCPNIForm.action`
- **Verizon**: `https://www.vzw.com/myprivacy`
- **T-Mobile**: `https://www.t-mobile.com/privacy-center/education/marketing-preferences`

For Women: Limit Your Health Data Tracking

Though I'm not aware of this actually occurring anywhere yet as of the publication of this book, women who live in states or countries that ban abortion are at risk if they use apps or services that track menstrual cycles or physiological indicators of fertility or pregnancy such as body temperature, weight, sleep cycles, and metabolism. That data could easily be obtained by law enforcement via warrant or subpoena (or it could just be given upon request, if the health tracking service gives itself permission to share your information), and used as evidence in a criminal abortion case. Such evidence would be particularly damning alongside other corroborating personal data such as Web search results, Web history, call

history, location / GPS history, and the content of text and email messages.

As convenient as it is to have your smartphone, smartwatch, or smart scale record and analyze your health data (which will almost certainly be sold and/or used to show you targeted ads), it's safer to record it by hand in an encrypted spreadsheet or in a paper notebook – if you need to record it at all.

Even if you don't have an abortion, a natural miscarriage could potentially lead to a criminal abortion charge based on evidence from recorded health data. If you seek an abortion in a place that criminalizes it, make every effort to leave no information footprints that could be used against you.

Removing Information From Search Engines

One of the most useful tools for scammers, spammers, and stalkers is the plain old-fashioned Web search engine.

Though there are many Web search engines (and many more will be created in the future), Google is by far the most-used as of the publication of this book. If you own or control the website (or an individual page on that site) that you want Google to exclude from its search index, or if you have removed personal information from one of your pages and you want Google to refresh the index, you must use the Google Search Console (`https://search.google.com/search-console/`). Other major search engines have similar webmaster tools.

If you don't own the website that is publishing your personal information, Google has a process for considering its removal through its Content Removal form, which you can of course find through a Google search, or at this URL:

```
https://support.google.com/websearch/contact/content_rem
oval_form
```

Google's policy is to comply with removal requests that fit any of these criteria:

- Explicit or intimate personal images
- Deepfake pornography

- If your name is associated with irrelevant sexual content (such as if your name appears in search results for "porn actors" or "Las Vegas hookers")
- Personally-identifiable information (anything that could be considered doxxing)
- Images of minor children
- Any personal information published on a site that requires payment for removal
- Nudity or sexual content that includes a person under the age of 18

If your intellectual property rights (copyrights, trademarks, trade secrets, licensing rights) are being violated, there is a separate process to request removal through Google's Legal Help system (the URL is too long to publish here; just search for it).

> ➢ NOTE: Requesting removal from a search index does not remove the information from the Internet. It just makes it difficult to find.

There are similar processes for removing information from other search engines; I leave it up to you to consult their documentation.

Removing Webpages From The Internet Archive

The Internet Archive (`archive.org`, also known as The Wayback Machine) is a nonprofit corporation that has the noble goal of building a digital library that encompasses the history of the public Internet, for the benefit of historians, researchers, academics, and the visually impaired. Consequently it also records webpages containing personal information, even after that information has been scrubbed from live websites. It also records all of the things people published online in previous eras that had vastly different moral cultures. Do you really want anyone to see the things you posted to LiveJournal or Tumblr when you were 15 years old?

The practice of silently recording snapshots of every page on the public Internet and making them available to everyone in the world is debatable from a moral standpoint. My belief, as a privacy advocate, is that everyone

should have the right to unpublish anything that they've published on the Internet, including all logs, archives, copies, and records. It will always be true that information that currently seems harmless may someday become harmful, and information that we believe to be private may turn out to be accessible to people who seek to harm us. The Internet Archive also does not know exactly what it is recording, so if your legally copyrighted or trademarked material (such as an ebook or photograph) has been illegally copied and published somewhere on the Internet, those copies will be archived in the Wayback Machine.

There are two actions you can take to stop the Internet Archive from recording and publishing your content:

1. **Modify your Web server configuration to prevent the Internet Archive's scraper bot from visiting and recording your content in the future.** You should consult your Web server or hosting provider documentation to learn how to do this (or use a search engine), but typically this is accomplished by creating a rule in the server's `htaccess` file (the Internet Archive has a history of refusing to honor the restrictions codified in a `robots.txt` file). Here's an example that might work (no guarantees!):[258]

```
RewriteEngine On

RewriteCond %{HTTP_USER_AGENT} archive.org_bot
   [NC]

RewriteRule .* - [R=403,L]
```

    a. If it is not possible to exclude the archive.org bot, then you can prevent it from recording a webpage by **gating** it (requiring a login or CAPTCHA in order to access it).

2. **Request that your content be removed from the Internet Archive.** If you're requesting removal of archived pages from sites you own or service accounts that you control (such as on blogging sites or social media), then send an email to `info@archive.org` with the following details: the URL or URLs of the material, the time period to erase from the archive, the time period during which

[258] *https://beamtic.com/internet-archive-blocking*

you had control of the site or user account, and any other relevant information.[259]

a. If you are requesting removal of illegally-published copyrighted or trademarked material, then you must also include the following: identification of the infringed work; an exact description of where the material is located within the Internet Archive collections (this may encompass more than just URLs in the Wayback Machine); your address, telephone number, and email address; a statement that the copyrighted or trademarked work was not authorized to be republished in that manner; a statement that the above information in your notice is accurate and that you are the owner of the copyright interest involved or are authorized to act on behalf of the owner; and an electronic or physical (scanned or photographed) signature.[260]

Requesting Deletion From Data Brokers

Most corporations collect personal data to augment their main income streams, but data brokers exist solely to profit from collecting and selling information about people; obviously they don't want to make it easy for us to opt-out. Fortunately state and national laws and regulations are making it increasingly difficult for many data brokers to harvest and store information, and to keep it when we want them to delete it. The laws of every nation and state are different and they often change; therefore I cannot provide exact instructions for every reader. Even among the 50 US states, laws can vary wildly, with California historically being the most restrictive for corporate data collectors.

Where required by law, data brokers provide opt-out instructions on their websites. Don't expect the process to be easy or simple – or if you choose to use a third-party service to do the work for you, it won't be cheap. I have some guidance on both the manual method and the automated method in the subsections below.

---

[259] *https://help.archive.org/help/how-do-i-request-to-remove-something-from-archive-org/*

[260] *https://web.archive.org/web/20231204015925/https://archive.org/about/terms.php*

Individual Removal

There are hundreds of data brokers. While there are also thousands of companies that collect personal data for large-scale marketing efforts, they're a lot easier to opt-out from because they'll tell you who they are. Verizon, for instance, will use its data hoard to market its services; to opt-out, just contact Verizon. For large-scale marketing, though, most companies will purchase leads from data brokers.

Opting-out is a long-term process that will continually consume some of your free time. Even if you manage to request deletion from every data broker, your information has already been sold to an unknowable number of companies and government agencies in the past, and they're allowed to continue using that data until you ask them to stop. Think of it like shutting off the faucet after the sink has already overflowed and flooded the bathroom; you've stopped it from getting worse, but there's still a lot to clean up.

1. Every time you receive junk mail, contact the company that sent it and ask to be removed from their marketing list. Sometimes they will tell you that they outsource their direct mail marketing, or that they use lists that they buy from data brokers. Take note of those third-party services, and contact them to opt-out.

2. Search for your name, email address, phone number, and home address on Google, Bing, DuckDuckGo, and any other search engines you want to include. When you search for each of those pieces of information, put quotation marks around the entire query so that you don't get any irrelevant partial matches (you want to search for the exact terms only, and don't want results for people whose details are similar to yours). The search results will be a mix of data brokers (mostly of the "people finder" variety) and spam sites that use clever programming to dynamically insert search queries into page titles or content (you can ignore those; there's nothing to remove). After clicking through to some of the results, you'll get an idea of which sites actually have your data, and which are just trying to fool you. When you land on a data broker that has your information, navigate its site to learn how to remove it or opt-out of data collection and sharing. Keep records of your opt-out requests; take screen shots of opt-out forms, and save any opt-out request emails that you send. Repeat this process every 30 days

to see if your requests have been honored. If they have not, then the company may be in violation of the law, its own written policies, or the policies of search engines that index those sites.

   a. If any of the sites you find ask you to pay a fee for removal, don't pay it. Instead, ask search engines to remove those pages from their indexes as explained in the "Removing Information From Search Engines" section earlier in this chapter. That won't erase the data, but it will make it impossible to find via Web search. Removal fees aren't just unethical, they're also often scams. You may end up paying the fee only to see your information return to that broker's database in the future.

3. Many data brokers do not publish partial records online for the benefit of search traffic, so a Web search won't lead you directly to them. Consequently you'll have to contact them on your own. Technology journalist Yael Grauer actively maintains a list of the most important data brokers along with opt-out instructions for each at this address:

`https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List`

Using a Removal Service

If spending hours filling out opt-out forms, making phone calls, and sending paper mail and email sounds like too much effort to you (it does to me), then you'll appreciate the fact that these paid removal services can do pretty much the same thing (and maybe more) for a one-time or monthly or annual subscription fee:

- **Incogni**: (`incogni.com`) Incogni is a data removal service developed by the VPN company Surfshark — so you know they take Internet privacy seriously. When you sign up for Incogni, you provide your information and assign power of attorney so that the service can monitor for your personal information and contact data brokers on your behalf. Incogni is one of the most comprehensive data removal services available, with 180 data brokers in its database (more than most competitors). It also has a user-friendly interface that is easy to navigate. One of the main

downsides to Incogni is that you don't have a good way to confirm if data has been removed after a request is sent.

- **PrivacyBee**: (`privacybee.com`) One of the standout features of PrivacyBee is its free risk assessment. You can see how much of your personal info is available, and decide whether you want to take action. You can also get breach monitoring with a free account. If you want proactive data removal (PrivacyBee continually searches for your information and contacts data brokers on your behalf), you'll have to upgrade to a paid account. While PrivacyBee's features are comprehensive, it only lets you enter information for one person (and one phone number, email address, etc.). If you want it to scan for multiple email addresses, for example, you'll have to get a second account.

- **DataSeal**: (`dataseal.io`) This service covers 136 sites that collect information, including data brokers and public records. DataSeal works similarly to the other data removal companies on this list, but it stands out for its stellar customer service. With DataSeal you can sign up for breach alerts and agency protection in addition to the standard data removal, which is a monthly subscription charge. Unlike other data removal services that you only hear from when there's a problem, DataSeal sends you weekly privacy and safety reports.

- **Kanary**: (`www.kanary.com`) Like PrivacyBee, Kanary offers a free edition of its product with limited features. You can track two names, two addresses, one username, one email account, and one phone number with Kanary's free tier. You also get three automated removals without having to pay (competitors will monitor for free but won't do any removals unless you pay). Kanary's scan covers Google search results plus 327 sites — many more than some of its competitors. The automated opt-out process only works for about 260 of those sites, however. The remainder can be removed through a higher service tier.

How to Handle Being Doxxed

Being doxxed is a terrifying experience. Someone publishes your full name, home address, the company you work for, or the school you attend, with

the intention of ruining – or even ending – your life. Before I go any further, it's important to draw a distinction between doxxing and the sale or publication of information stolen in a data breach. Doxxing is targeted at a single individual; publishing that person's various personal and private details with the intent of enabling many other people to cause havoc for him or her at work or school, and at home. By contrast a data breach is not usually intended to cause harm except perhaps to the company that it was stolen from, though it can certainly be used as an information source for an act of doxxing.

With that in mind, the typical doxxing scenario fits this basic paradigm:

1. An "extremely online" person (the doxxer) is offended by another person's words, actions (either online or in real life), or political affiliation(s); or is envious of his or her Internet fame.

2. Assuming the target is using some kind of screen name or online handle (this step is unnecessary on services where people use their real name, such as social media, a Web forum, or a game like iRacing), the doxxer works to discover who their target is by:

    a. Searching for identifying clues in the target's post or chat history.

    b. Asking other users if they know any information about the target, such as their name, location, profession, or social media accounts.

    c. Analyzing the target's username for clues as to their identity (their name, initials, birth year, or any indicator of their age, location, school, or profession).

    d. Searching the Web for the target's username, since many people use the same online handle across multiple services and platforms, including their email address.

    e. Digging into technical information sources to determine the target's IP address, which can be traced to a specific ISP and an approximate geographic location.

3. Once the target's name has been discovered, the doxxer will search the Web, Dark Web, and public records to learn his or her home address, and any other personal information. This information can

also easily be sourced from any of the multitude of data breaches that have occurred, and continue to occur. A particularly motivated (or simply wealthy) attacker could even purchase personal data legally from a data broker.

4. The doxxer publicly posts what they've found, usually on a Web forum or social media site, along with a "good reason" why his or her chosen victim should be punished. Sometimes this "good reason" is a total falsehood; it is common, for instance, for Gamers to claim that their target said something racist, hoping to attract the attention of anti-racism vigilantes. Sometimes there is no "good reason" – the doxxer simply wants to disrupt a popular Twitch or YouTube streamer while they are broadcasting; or harass a disfavored celebrity, politician, or other public figure.

What happens next is unpredictable. Perhaps nothing; the doxxer may fail to motivate others to attack the victim, or the dox post will be removed by moderators before it can do any harm. Often, though – as I have shown in several of this book's case studies – the results range anywhere from "annoying for a little while" to "completely ruined someone's life." In the early days of doxxing it was common to order a large number of pizzas to the victim's house to be paid on delivery, or to make prank (landline) phone calls to their home in the middle of the night. Today the goal is typically to get someone to resign from their elected or appointed office, fired from their job, expelled from their school, assaulted or murdered by a deranged psychopath, or shot by the police (swatting). Modern attackers will also call the police and issue threats of terrorism in the victim's name, or call the victim's utility providers and have their services shut off.

The doxxer is not always one of the attackers; sometimes he or she simply wants to throw some raw meat into a pack of Internet vigilantes and hope for the worst. Sometimes there is no doxxing at all; the doxxer simply uses the information they've collected to attack the victim directly, or he or she shares the information privately with a group of "extremely online" psychopaths who take pleasure in harming others (usually through swatting).

I've already given you all of the relevant advice for making doxxing as difficult as possible. It's never impossible, though, especially for a motivated attacker. The most common targets for doxxers / swatters are politicians and other appointed or elected officials (such as judges,

prosecutors, and school board members), celebrities (musicians, actors, online influencers), journalists and pundits, authors, streamers, and anyone who is the focus of a news story.[261] If you are at all in the public eye, then you're at an elevated risk of being doxxed. Ordinary non-famous people are no less vulnerable to doxxing under certain circumstances, though. My advice:

1. If you participate in any game or online service where you will be known by a handle or pseudonym, don't choose a username that identifies you in any way, and don't use the same one across multiple services. If possible use an auto-generated username or a random string of letters and numbers (you can use your password manager to generate one for you).

2. Don't give anyone a reason to dox you. Don't grief other players in online games, don't start "beefs" or feuds on social media, don't be antagonistic toward anyone online no matter how anonymous and untraceable you think you are, and avoid controversial topics when expressing your political or social views anywhere on the Internet. In other words: don't be a jerk. Act as though you're already doxxed. People have been physically attacked and even murdered over things they've done in online games. One couple in Milwaukee has been swatted more than 40 times since 2018, simply because one of them tweeted that he'd never found the late comedian Norm Macdonald to be funny.[262] The Internet is full of psychopaths; don't draw their attention.

3. Be proactive. Ask someone in your employer's HR department if there are policies and protections against harassment from doxxing. Many police departments now have systems in place to mitigate swatting attempts; check your county Sheriff's office and/or city police department's website to see if there is an anti-swatting registry. Even if you don't currently qualify for it, you'll be glad you know it exists if you get doxxed in the future.

As I've illustrated, though, it's not the doxxing itself that is the real harm; it's what people do with that information once they have it.

---

[261] https://www.bbc.com/news/world-us-canada-68297349
[262] https://www.nbcnews.com/news/us-news/fbi-formed-national-database-track-prevent-swatting-rcna91722

If you've been doxxed, unless you are using a service that actively monitors the Web for your personal information (as explained in the previous section), most likely you will only find out about it when you've been targeted for an attack. Here are the steps you should take if that happens:

1. Don't give the attacker what he or she wants most: a public emotional reaction. A victim's pain is a psychopath's pleasure. If you post about being doxxed on social media, or complain about it on your livestream or podcast, or go to your local newspaper or TV station to ask journalists to report on it, then the doxxer knows that he or she has gotten to you and will continue (and probably escalate) the harassment.

2. Contact your local police department. Tell them that your personal information has been published online, and that you're concerned that it will be used to swat or otherwise harass you. If you've already been harassed or threatened, report it.

3. Save and document all forms of harassing messages (emails, DMs, IMs, chats, text messages, voicemails) with screen shots, recordings, and URLs.

4. Find the source of the dox. If it's on a website or service that prohibits doxxing (nearly all of them do), report the post to the moderators or admins immediately. If that doesn't work, contact the website's hosting provider; in most Western nations, hosting providers prohibit this activity.

5. Speak to the people you live with – family, roommates – about the incident so that they know what's going on, to look for suspicious behavior, and to understand that your home may be visited by heavily armed police who think that a violent crime or act of terrorism is in progress.

6. If you have dogs, prepare to put them in a crate or pen, or lock them in the cellar or a bedroom if the SWAT team shows up.

7. Speak directly to your boss and your HR representative or University dean to let them know that you're being targeted for harassment.

If you follow these steps, most likely your doxxed information will soon be removed from the public Internet, and the attacker will move on to a

new target. Over the past few years, police departments, the FBI, and state and national governments have grown to understand the seriousness of doxxing and swatting, and are actively creating systems, programs, policies, and laws to combat it. As a result, several "serial swatters" – people who have committed multiple acts of swatting – have been arrested and sentenced to prison.

Chapter 7: The Hidden Costs of Privacy

The institutions of the modern world are obsessed with collecting and using people's personal data for various reasons; that is why they make it difficult for us to protect our privacy. As I've mentioned a few times already, sometimes you are *forced* to surrender some of your personal information. However, there are a lot of scenarios in which you aren't legally required to hand over your information, but you'll be pressured or bullied into doing it anyway. In the real world this most often manifests as low-level enforcers who tell you "I'm just doing my job," and cannot answer your questions about how your personal data will be handled, stored, and used. In the digital realm, companies that rely on personal data collection for profit will try to sabotage your privacy efforts in a variety of ways. In the sections below, I explain the most common scenarios in which you'll be hassled or hamstrung by protecting your privacy, and some methods for handling it.

The Gatekeepers of "Our Policy"

When someone who isn't in law enforcement says "I need to see your ID," and you refuse, you'll often be unable to proceed with what you want to

do. Sometimes you can fight it, and sometimes you can't. Laws in most jurisdictions require that you show government-issued photo ID (passport or passport card, driver's license, non-driver's ID, or military ID) to purchase age-restricted products such as pornography, alcohol, cannabis, or tobacco (or more broadly: products containing nicotine). Some US states require (or strongly incentivize) businesses to electronically validate (swipe or scan) IDs, which can lead to information collection as I explained in Chapter 3. I encourage you to choose to patronize businesses that don't swipe IDs, but this may not be possible in some places.

There are ways to dodge the swipe. First of all, you can simply demand that it not be swiped. Shockingly, some people will tell you that they won't swipe it, then they'll do it anyway right in front of you; others will tell you that swiping is the only option. You're legally required to keep your driver's license in good condition, so you cannot use a magnet to ruin its magnetic stripe, or a permanent marker or sharp object to scratch out its printed barcodes, but you can place a sticker over them to prevent unwanted scanning (if law enforcement needs to swipe the license, you can just remove the sticker). Another way to dodge the swipe is to use a valid ID that is not a driver's license, such as a passport, passport card, or military ID because many businesses that sell age-restricted products are only configured to scan driver's licenses (this is never a guarantee, though). Unfortunately clerks and bartenders may not be allowed to accept an ID if it can't be scanned or swiped, even though it is a valid government-issued card; businesses are generally within their rights to refuse to sell age-restricted products if the employee isn't comfortable with the ID the customer presents to them. My advice is: fight it whenever and wherever you can, and make your position and opinion known, but this probably isn't the hill to die on. Ultimately the best way to fight information collection via ID swiping is (aside from taking your business elsewhere) in the voting booth by supporting politicians, propositions, and legislation that protect privacy and data rights.

The most common example of unreasonable information collection unrelated to age-restricted sales is the dentist's or doctor's office, where you will likely be asked to hand over your driver's license to be copied or scanned. The office worker charged with this task probably only knows that this is what the boss told them to do. Some may say that it's a requirement of dental insurance providers (according to my research, dental insurance companies only require service providers to verify the

identity of the insured patient, not to scan, photograph, or photocopy driver's licenses or other government-issued IDs); some say that "it's our policy" (which you are not legally required to submit to; many businesses have policies that aren't legally enforceable – or even legal at all – and when they violate your standards, you can and should make it "my policy" to go elsewhere for service); some may even say that it's Federal law to digitally record your ID (it is not).[263][264] I'm not sure which law those people are referring to, but the closest thing I could find is the US FTC's Red Flags Rule, which aims to reduce identity theft and fraud by requiring creditors and financial institutions (neither of which is your doctor or dentist, unless you're applying for credit directly from or through them) to verify a customer's identification if there is any doubt as to the legitimacy of their personal or financial details. The Red Flags Rule does not recommend copying, photographing, or scanning government-issued IDs for this purpose.[265]

This is not a minor concern. According to the American Dental Association (ADA), loss or theft (and I'm comfortable with adding "sold without ensuring that data cannot be recovered from it") of unsecured devices (computers, mostly) is a major cause of data breaches in dental practices.[266] Furthermore, even if your dentist or doctor has excellent information security, there's a good chance that they rely on potentially vulnerable third-party service providers (such as the ones I covered in Chapter 3) to store or process patient information. I recommend that you show your ID, but demand that it not be copied, scanned, swiped, or photographed. There is absolutely no good reason to allow your ID to be recorded in that fashion.

---

[263] https://www.medicaleconomics.com/view/how-handle-patients-who-dont-have-identification

[264] https://revenuecycleadvisor.com/news-analysis/qa-photo-id-requirements-patient-appointments

[265] https://www.ispartnersllc.com/blog/what-is-the-ftc-red-flags-rule-and-who-must-comply/

[266] https://www.ada.org/resources/practice/dental-insurance/dental-insurance-resources/dental-insurance-frequently-asked-questions

Hassles From Companies With Bad Information Security

Some legitimate e-bills, especially from medical service providers and labs, violate all of the rules I've suggested to avoid phishing: the originating email address does not match the company's domain, the payment link is obscured and/or leads to an unfamiliar third-party payment site, and if there's an attached PDF it may require a password that is your date of birth or other personal information. Every one of these things is a red flag, yet the email may be legitimate. This is a perfect example of why switching to paper billing is usually safer; while a thief *could* send you a fake paper bill, the cost involved and added risk (the US justice system takes paper mail fraud much more seriously than email fraud, but I hope this will change in the near future) make it unrealistic.

So if you follow my advice on phishing avoidance, you could end up deleting a legitimate bill, invoice, or account statement. To pay the bill, you'll have to go to the company's official website and either pay through that (if you can – sometimes you need account numbers or other information from the PDF that was emailed to you) or call. Scammers and thieves succeed in part because these kinds of companies are so badly educated in anti-phishing practices, and make it so difficult to pay bills in secure ways.

CAPTCHA Hell and VPN Blocking

In Chapter 2 I told you to always use a good, privacy-focused virtual private network (VPN) on all of your connected devices. This will hide your IP address (and therefore your location and possibly other information that can be re-identified by data collectors and doxxers) and filter out a lot of data-seeking code and ads in websites, apps, and emails. Unfortunately it may also introduce some inconvenience and occasionally prevent you from accessing certain sites or services.

The most common anti-VPN strategy that data collectors use is to force you to go through **CAPTCHA hell** (the process of repeatedly making you do useless, aggravating, time-wasting work ostensibly to prove that you are a human and not an automated program; however this may also be used to discourage people from using VPNs). CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans

Apart, and it was invented to prevent people from using software to access services intended for humans; most notably to prevent brute-force attacks. CAPTCHA manifests as an act of meaningless work that you are asked to perform, for instance:

- Clicking a checkbox to verify that "I am human."
- A segmented photo in which you have to click the tiles as instructed, such as to "select all fire hydrants" or "select all bicycles."
- A request to look at a distorted image that shows an alphanumeric code, which you must type into a text field.
- Moving a slider to put a graphical puzzle piece into the correct place.
- A simple math problem.

VPNs encrypt and relay Internet traffic through many different servers in a wide variety of locations so that data collectors can't know your IP address; good VPNs also filter out junk traffic like tracking code and ads, when possible. Unfortunately modern Web servers are quick to isolate suspicious activity from a given IP address because hackers use VPNs to try to obscure their location. As I explained in Chapter 3, hackers often use scripts for brute force tactics, but they can also use them to scrape a page that contains user-specific information, or to execute a DDoS attack. Once a service provider detects suspicious traffic from a VPN node, it enables CAPTCHA routines for all traffic originating from it. While this usually blocks most (but not all) evil hacker scripts, it also puts a burden of inconvenience on regular people who just want to protect their privacy.

Unfortunately CAPTCHA isn't perfect. Sometimes it works as intended and you pass the test and go on to the site as usual, but often you'll find yourself trapped in CAPTCHA hell: an unending series of CAPTCHAs that never let you pass no matter how many times you correctly click on all the bicycle tiles (or whatever) in the images. In these instances the site's developers or the third-party firewall services that they use are specifically trying to thwart VPN users (or sometimes to thwart competing VPN services, if they offer their own), even when they're not hackers. The hope is that you'll be so annoyed by this nonsense that you'll shut off your VPN

and allow them to collect your data. I reluctantly admit that occasionally this is indeed necessary.

The best VPNs actively try to counter anti-VPN tactics by periodically changing the IP addresses of their nodes, and quickly blocking any activity that is obviously hacker-related. Therefore, sometimes you can simply connect to a new VPN node and dodge CAPTCHA hell, but even if you have to turn the VPN off for one important site (such as your bank or brokerage), you're still blocking all the invasive junk everywhere else you go. Besides, doesn't your bank or brokerage already have much more important personal information about you than can be recorded through trackers and cookies?

2FA Hell

Related to CAPTCHA hell is **2FA hell**, in which you are asked for a secondary authentication method every time you use an app or website while connected through a VPN. This is by no means a bad thing – I actually think it's a good idea, even if it's inconvenient sometimes. What I don't like is when those same sites and apps don't ask for secondary authentication when you *aren't* using your VPN.

Missing Features and Device Lockout

By refusing to hand over your personal information and agree to invasive privacy policies, many of the advertised features of connected devices will not be available to you. The most common example is modern TVs that embed a third-party software platform from Amazon, Google, or Apple. The first time you turn the TV on, you'll be asked to log into or create an account with one of these companies, then agree to abide by software licenses and privacy policies. If you decline, you'll find that your TV won't be able to do many of the things you expected it to. You can usually create a dummy-information account to bypass this, though you won't be able to use any mobile apps associated with the TV if you aren't using the same account between your mobile device and the television.

New cars also embed third-party software, and car manufacturers are increasingly collecting a creepy amount of information about owners. If you choose to decline the agreements, some or all of your car's

computerized features (such as GPS navigation, remote start, media players, and mobile device connectivity) may be disabled.

In some cases you may discover that a device you purchased may not work *at all* unless you agree to disagreeable terms, such as video doorbell systems, video and audio recording equipment, media streaming devices, toys, and tools. In 2016, John Deere instituted a mandatory "agreement" that forbade the owners of its farm equipment from performing any repairs; it was forced to relent in 2023 after years of overwhelming pressure from customers, consumer rights advocates, and various branches of the Federal government (including an executive order from President Biden).[267]

Until such a time as Federal regulations heavily restrict corporations' ability to collect our personal data and lock us out of the products we purchase if we don't agree to disagreeable licenses and policies, we will have to thoroughly research every available option before buying nearly anything new, and the most privacy-friendly products will almost always be the most expensive because they aren't subsidized by personal data collection.

No More (Upfront) Discounts

At first, opting-out of rewards and discount programs appears to increase the price of many of your retail purchases. If you think about it more deeply, though, is the upfront savings really worth the long-term cost – and is it even real at all? Aside from the fact that your personal data will be used to continually push you into buying extra things (and making choices that optimally benefit the retailer at the expense of the customer), consider the fact that many retailers have adopted dynamic pricing schemes, so you'll never know whether the "discount" you're being offered is truly a good deal – in fact the price of any given product may even be specific to each customer, set by personal data-driven algorithms that determine the maximum amount of money each shopper is likely to pay for it.[268] In the recent past, retailers have been caught promoting fake sales by raising prices and then "discounting" them back to their original prices to make it

[267] *https://arstechnica.com/tech-policy/2023/01/john-deere-relents-says-farmers-can-fix-their-own-tractors-after-all/*
[268] *https://www.washingtonpost.com/business/2023/11/21/fake-sale-deceptive-pricing/*

look like they're limited-time bargains, and a 2022 analysis of Black Friday deals at major retailers found that 98% of the advertised items were either cheaper or the same price at other times during the year.[269][270]

Paying For Formerly "Free" Services

In Chapter 2 I advised you to migrate from "free" online services to more secure and privacy-focused alternatives. Those services cost money – not a *lot* of money by Western middle-class standards, but I wouldn't expect someone who is struggling to pay the rent to willingly take on another monthly or annual bill that isn't critical to survival. The impoverished and near-impoverished have more important concerns than whether Google's algorithms are reading their email to deliver more effective ads (which largely will be blocked anyway, if they're using a privacy-focused browser like the ones I recommended).

Services like Proton (which includes email, file storage, calendar, password manager, VPN, and a thin-client software suite roughly comparable to Google Workspace) are priced according to their true cost to develop, deliver, maintain, and support. That should give you a rough estimate of the bare-minimum amount of money that "free" service providers (or their advertisers) anticipate extracting from you while you use them; in fact your personal data is probably worth more than that to them because there's no profit margin baked into Proton's pricing.

If you can afford it, I think it's far better to pay a little bit of money for high-quality services that protect your privacy than to use "free" alternatives that have unknowable open-ended costs powered by your personal data.

[269] *https://www.msn.com/en-us/money/companies/target-s-fake-black-friday-deals-exposed-online-as-experts-weigh-in-on-sales-strategy/ar-AA1kAwS4*
[270] *https://www.which.co.uk/news/article/98-of-black-friday-deals-werent-worth-buying-last-year-aoIJw3j40Sou*

Chapter 8: How to Be Found (the "Right Way")

I've spent most of this book telling you how to take back your data rights and regain your privacy by reducing the information that you expose, provide, and validate. But what if you actually do want to be findable on the Internet? This isn't an unreasonable or uncommon scenario, and there are safe ways to do it.

Nearly everyone *does* want to be found by certain people under certain circumstances, but privacy often feels like a firehose that's either on full-blast, or completely shut-off. That doesn't have to be the case. In this chapter, I'll show you some ways to be findable on the Internet while maintaining your privacy and minimizing your risk of harm.

Metadata Management

Every object on the Internet – webpages, images, videos, MP3s, documents, files – has a hidden layer of **metadata** (data that describes other data). Metadata enables files to be sorted, indexed, searched, and described in human terms. Most metadata is automatically generated based on freely-discoverable facts such as how many words are in a document, the resolution and color depth of a digital photo, and the exact date and

time when an executable program was uploaded to a file server. Some forms of metadata are entirely supplied by humans: hashtags, for instance, are a kind of metadata that associates specific topics with a piece of Internet content. Regardless of how it is created, nearly all metadata is human-editable.

While the number and maximum length of metadata fields varies among digital objects, some information is universal: the date and time a file was created, uploaded, or modified; the size of the file in terms of disk space (in bytes); and local access controls (whether the object is readable, writeable, and able to be deleted by specific user accounts, user groups, or everyone).

Audio files typically include the artist or band name, track number (if it's part of an album), track title, length, date of production or release, genre, and potentially dozens of other metadata fields that are reserved for specific media players, music download services, and other audio-specific platforms and apps. For instance if you purchase an MP3 from Google Play or Amazon, those companies will add special metadata tags that identifies them as the licensor, marks the file as being protected by copyright, and specifies your user account as the person who "owns" the file (meaning you've paid for a license to download and listen to it). If you then share that MP3 with someone else, the media player or music service he or she uses may check for those metadata tags and refuse to play the file because it was only licensed to you.

Documents (including spreadsheets and all other "office" files) typically include the author's name, the names of other contributors, style specifications (fonts, page dimensions, etc.), and may also include margin comments (even if they've been deleted) and a full history of every change made to the file. There have been several newsworthy scandals sourced from metadata stored in Word documents and PDFs that revealed information that the author believed had been permanently deleted or hidden. If you are preparing a document for public release, be sure to review its metadata (in Word, Acrobat, LibreOffice, or whatever you use to create documents) beforehand and delete or correct any unwanted metadata.

Images and videos also can have dozens of metadata fields to specify a wide variety of image properties, plus information about the hardware that originally captured the photo, and the software used to modify it. Most

importantly, smartphones often put GPS coordinates into image metadata to identify where in the world that photo was taken (you probably want to remove that from most images, especially if they were taken in your home). Before you post any image or video publicly, review its metadata with an editing tool (such as Photoshop, GIMP, Premiere, or whatever app you use for image or video editing) and ensure that all unnecessary details are removed, and that all of the information that you want to disclose is correct and complete.

To a limited extent, you can edit the metadata of any file on a PC by right-clicking it in your file manager and selecting **Properties** from the context menu. There are also some open-source programs that specialize in modifying file metadata:

- **Music files:** MP3TAG (https://www.mp3tag.de/en/)
- **Images and videos:** ExifTool (https://exiftool.org/)

Metadata isn't necessarily bad. It's often a good idea to identify yourself as the author of a document, so you may want to leave that in, or correct it if it's wrong. You may also want to identify yourself as the photographer or subject of an image, the voice actor or musician featured in an audio file, or the person featured in a video. If you are producing something for a client or your employer, you may want to specify the company name as the file's owner rather than yourself. Most files have metadata fields where you can put an email address or URL, which may be useful professionally. Lastly, if you use an online handle or pseudonym (there's more information on this topic in the next section), be sure to use that instead of your real name in all file metadata.

Pseudonyms and Selective Disclosure

Some things about you may feel private, but legally are not. For instance your visual image, unless you control the copyright; anyone has the right to take a picture of anyone else in public, and there are many private and public security cameras out in the physical world, constantly recording.

Your legal name is something that you can't truly hide or prevent others from publishing, but you can obscure your identity with nicknames, professional names, or online handles that don't correlate to your actual identity. For instance, do you know the real given names of The Weeknd,

John Wayne, or Lady Gaga? Offhand perhaps not, but since this is public information, you can easily search the Internet and find the answers: Abel Makkonen Tesfaye, Marion Robert Morrison, and Stefani Joanne Angelina Germanotta, respectively. These people's given names are not secrets, but there is little benefit in knowing or remembering them. If you search Spotify for "Abel Makkonen Tesfaye," you will probably end up (in a roundabout way) finding The Weeknd's music, but you'd be better off simply searching for "The Weeknd" because that is the artist name embedded in all of the song, album, and playlist metadata.

If you do anything intended for public consumption such as blogging, streaming, or journalism, using a pseudonym will provide a layer of abstraction between your personal and professional (or amateur) life, and make it easier for people to find your work. Obviously this isn't an ironclad method of protecting your identity online, but it provides a clear avenue for people to interact with you professionally while also directing them away from your private details; it's approximately the same level of obfuscation as relegating all of your professional activity to a limited company or LLC (and if you're serious about this from a business standpoint, then it may be a good idea to incorporate your pseudonym as an LLC and perhaps even seek copyright and/or trademark protection for it).

There are certain things that you cannot keep secret, but you can take some degree of control over them:

- If you are known publicly by a professional name, pseudonym, or persona, avoid press interactions "out of character." For example, for most of the late comedic actor Paul Reubens' career, he would only do interviews in character – with full costume and makeup – as Pee-Wee Herman.[271] This enabled Reubens to remain relatively anonymous whenever he was out in public – no one knew what he actually looked like, and many people weren't even conscious of the fact that Pee-Wee Herman was a fictional person.

- Use your pseudonym for your website domain name, your LinkedIn profile name, and other public presences.

[271] *https://www.imdb.com/name/nm0000607/bio/*

- If you don't use a pseudonym or professional name, then create separate email addresses for personal and professional purposes. For instance you might use `johnsmith@example.com` as your public email address that you print on your business cards, and `JS@example.com` as your private "friends and family only" email account that you can sort separately in your email app.

- For your websites, use your registrar or hosting provider's anonymizing service that obscures your domain ownership and contact information.

- As explained in Chapter 2, use an email masking service whenever you need to send a message to someone without revealing your private email address.

- Also as explained in Chapter 2, obtain a Post Office box or third-party mailbox or package-receiving service address, and use that as your mailing address for everything you are legally allowed to.

- Use a separate phone number for professional purposes, and ask your friends and family not to reveal your personal cell phone number to anyone. If you don't want to use a separate cell phone or virtual SIM for your public-facing phone number, then you can use a voice over IP (VoIP) service to obtain a virtual phone number that can receive voice calls, voice mails, and text messages. If you take that route, be sure to choose a VoIP provider that doesn't collect your personal data.

- Dummy accounts on social media can be a useful red herring. For instance if your school or employer asks you for your X handle or Facebook page so that it can be vetted and monitored, you can direct them to a locked-down, barebones, boring account associated with your real name instead of the one that you actually use (though you'll have to use some sort of pseudonym for your main account).

- Don't give permission for your personal contact information to be included in church directories, school alumni listings, or other sites that would associate it with your full real name.

Your Freelance Portfolio

Your work history is private information, but if you're a consultant or freelancer you may want to disclose (with permission) past clients and projects for your professional portfolio. There are two sides to this: protecting your own information, and protecting your clients' information.

The first thing you should check / change is the metadata on all of the files you want to publish online. Ensure that the copyright owner (whether that be you or your client) is properly identified, and that you're credited as the creator. It's a good idea to correct any other metadata as well, such as the date of publication.

If you want to present your previous copyrighted or personally-identifiable work in your professional portfolio (for instance if you've created some employee bulletins for Walt Disney World employees, but you don't want to or aren't allowed to publish them publicly), you can depersonalize your work without sacrificing its artistic value. Text content can be replaced by *lorem ipsum* filler text, and logos can be replaced by generic shapes. No matter how much you obfuscate a file for your portfolio, though, be sure not to use any images or other material that are owned or licensed by the client.

In terms of publishing, the only truly safe and trustworthy platform for your material is your own website. While there are various services that offer portfolio or reel (for actors) services, mostly they are just basic file and Web hosting services. Hosting your own material, rather than linking out to DeviantArt or Google Docs or some other service, also makes you look more capable and professional.

Chapter 9: The Enshrinement of Personal Data Rights

You now have the tools and knowledge to protect your privacy and reasonably safeguard your information in a world where nearly everything is searchable. If you've left any work from Chapters 1, 2, or 6 undone, I urge you not to put it off any longer. Do it right now, or schedule some time on your calendar to do it soon. Chapter 9 will still be here when you're ready to continue.

Assuming that you've taken all the actions and precautions that I've recommended, the final step is to solidify the idea of **personal data rights** – that you, as a citizen, have the right to maintain your privacy and be free from the pervasive manipulation of propaganda and marketing driven by personal data collection. The rarely-cited 9th Amendment to the US Constitution – part of the Bill of Rights – lays the groundwork for this:

> *"The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."*

In other words, the Founding Fathers knew that there were potentially other "inalienable rights" (to quote the language in the Declaration of

Independence) that they had not yet encountered or conceived of, so they explicitly stated in this amendment that the Bill of Rights was not a complete list, and that the specific rights they defined should not override or prevent the establishment of others in the future. Arguably this is the most important element of the Bill of Rights, because it enabled many more amendments to define new rights as they came into public consciousness.

Rights may be granted – in the Constitution, case law, or legislation – but they still must be constantly defended in order to ensure that they are guaranteed. In this chapter I'll show you some ways that you can help establish (and defend) the principles of personal data rights in your own life and in your sphere of influence.

Vote With Your Attention and Your Clicks

Everything you click or tap on in an app or website is being recorded, if not by cookies, trackers, and advertising code, then by Web server logs. Even when you're using a VPN, your activity still tells the company that owns the app or website what is of interest to visitors. No metric is more important on the Internet than the number of clicks something receives.

The more you interact with ads, the more you teach advertisers how to develop them more effectively, even if they aren't able to customize them based on your personal data. I don't want to say "never click on an online ad;" rather, I want you to treat every click and tap as a conscious vote for what you want to see more of in the future, whether that's ads, news stories, YouTube videos, app downloads, webpages, podcasts, or app features. If you consider a particular service, corporation, or content creator to be unethical or immoral, don't vote for them with your attention – refuse to give them a click.

In an ideal future where personalized advertising is universally banned and personal data collection is minimized, the Internet will evolve as it did before it was corrupted by mass data collection: meritocratically, where the best content and the most trustworthy sources will prevail.

Allow "Good" Data Collection Sometimes

Once data's been collected, you never know how it will be used in the future (including if it'll be stolen and used to harm you), regardless of promises made at the time it's collected.[272] As evil as tech companies can be, occasionally they do something that is designed solely to benefit the public without any ulterior motive. Some notable examples of this are:

- When there is a mass shooting or natural disaster, Meta will ask Facebook users who were known to be in the area at the time to click a button that lets their Friends know that they're safe. I don't see any harm in participating in this feature because Meta already has your personal information and is actively tracking your location via its app, so you aren't truly revealing anything personal or secret aside from the fact that you're alive. Of course, you could also just make a public Facebook post that says you're safe.

- During the COVID-19 pandemic, Apple and Alphabet joined forces to use their smartphone platforms to help contain the spread of the virus.[273] Various public health agencies in local and national governments attempted to create their own smartphone apps that would enable rapid contact-tracing, but (somewhat ironically) the privacy safeguards for Android and iOS apps fundamentally prohibited them from using device features that would enable an adequate degree of location accuracy, and from sharing personal information about each potentially infected user. Apple and Alphabet, however, were able to develop an "exposure notification" system common to both platforms that protected users' identities while providing a high degree of location accuracy. Users were given the choice to opt-in to this platform by manually downloading the app; it would then give them the option of securely and anonymously reporting when they'd tested positive for COVID-19, and notified other users if they'd been in close proximity to someone known to be infected.

- Alphabet developed a feature in Google that attempts to detect, based on search queries, if someone is considering suicide or self-

[272] *https://www.forbes.com/sites/forbestechcouncil/2020/06/24/data-collection-the-good-the-bad-and-the-ugly/?sh=473740a645fa*
[273] *https://www.cbc.ca/news/science/apple-google-covid-app-1.5577166*

harm, and prioritizes legitimate non-monetized self-help resources in the search results. If you're using Google, then you're already consenting to a certain amount of personal data collection, so this isn't anything extra to be concerned about from a privacy standpoint.

As I explained in the 23andMe case study in Chapter 3, corporations aren't always completely honest when they tell you that they'll use your data only for noble purposes. 23andMe, for instance, grants itself the right to use customer data for "product development" purposes when they opt-in to sharing it for "research." At that point you've already given the company your data, though, so you're already at risk to a certain extent. That doesn't mean you should consciously make it worse, and no one's life is at stake if you choose not to participate; the potential positive impact of sharing your genetic data with unknown third-parties via DNA-testing services is low, but the risk to your privacy is high.

Stay Current

This book represents a snapshot of history, specifically early 2025. Tomorrow some new technology or regulation may fundamentally alter the way personal information is collected, used, and shared. While significant news stories on the topics of privacy and data rights regularly make it to the mainstream news media, I recommend that you follow them more closely by adding these sources to your information diet:

- **EFFector:** https://www.eff.org/effector
- **Privacy Not Included:** https://foundation.mozilla.org/en/privacynotincluded/
- **Data Breach Today:** https://www.databreachtoday.com/

Don't Reveal Secrets – Yours and Others'

As I explained in Chapter 3, there are many different types of thieves. While digital thieves can use software to automatically try to break into people's accounts, and can purchase caches of stolen information on the Dark Web to try to commit identity fraud, other thieves are opportunistic. The most desperate among them might smash the window of a random

parked car to rummage through its contents hoping to find something of immediate value, but most will at least look through that window first to see if there's anything worth stealing. Similarly, burglars rarely break into homes without knowing who and what's inside them beforehand. Lastly, some people do not become thieves until presented with an opportunity to steal something of extraordinary value.

The people close to you don't always know what is and isn't a secret to you. For that reason it's best not to reveal any information that would make you a target for a thief if he or she were to overhear it in a social setting. Don't brag about owning anything that someone would be motivated to steal:

- A safe or lockbox, no matter what is in it
- Guns and ammunition
- Expensive jewelry
- Precious metals
- Cash
- Drugs, both legal and illegal
- A coin collection

Likewise if your friends and family own any of these things, don't brag about them to anyone – or at very least, don't reveal any personal information that would help an eavesdropping thief figure out who you're talking about. Beyond that, there are some non-obvious pieces of information that you shouldn't reveal about your friends and family members (or yourself):

- They have fallen victim to a scam
- They have been robbed in the past
- They will be away from their home for a period of time (in the hospital or on vacation)
- They, or the people they live with, have an addiction problem

Again, if you absolutely cannot stop yourself from telling stories at parties, then at least don't reveal any identifying information about the people you're referring to, and change names and other details so that no one can figure out who you're talking about simply by looking at your social media connections.

Vote for Personal Data Rights

I'm not going to suggest that you become a "one-issue voter" because that's always a Faustian bargain, but I do encourage you to evaluate all politicians and laws that are on the ballot before you vote for them. If a politician hasn't made a public statement or has no voting record on data rights issues, call or email his or her office and ask what the candidate's position is. Politicians being what they are, they may tell you one thing before the election and do something different later, but at least you're making the best and most informed decision that you can.

While privacy protection and data rights often share space with other issues – advocates for gun rights and abortion access, for instance, also desire greater privacy – sometimes they are inherently at odds with them. For instance a politician that is "pro-business" probably will act in favor of corporations collecting and using your data, and act against privacy and data rights, though it is certainly possible to only favor businesses that do not violate their customers' privacy.

Not all laws and regulations are what they appear or purport to be. Corporate lobbyists are masters of media spin, and can make a piece of anti-privacy legislation seem beneficial through clever language and media propaganda. When threatened, corporations that profit from exploiting personal data may raise the prospect of economic harm via layoffs or loss of tax revenue if a piece of pro-privacy legislation passes. Ultimately I feel a legitimate business should be able to make a profit without collecting and using personal data, and companies should not collect any personal information beyond the minimum necessary to serve its customers. Data collection, regardless of purpose, eventually leads to data breaches.

The European Union already has extensive pro-privacy laws in the form of the General Data Protection Regulation (GDPR), enacted in 2016.[274] Its main provisions are:

- Companies must give explicit notice to someone when collecting their personal data, explain exactly what it will be used for, and obtain their consent to use it.
- All personal data must be encrypted at rest.
- EU citizens have the right to request the information a company has collected about them, and the right to demand that it be erased.
- A company that suffers a data breach must notify the relevant EU authorities within 72 hours of discovery.

These rules apply not only to EU-based companies, but also to any foreign company that does business in the EU. Google, for instance, has already been fined 44 million Euros for violating the GDPR.[275]

In 2018, the state of California passed the California Consumer Privacy Act (CCPA), which gave California residents similar protections to the GDPR:[276]

- The right to know about the personal information a business collects about them and how it is used and shared.
- The right to delete personal information collected from them, unless the business is legally required to retain that information (such as for KYC purposes).
- The right to opt-out of the sale or sharing of their personal information.
- The right to non-discrimination for exercising their CCPA rights.

In 2020, two additional privacy protections were added to the CCPA:

---

[274] *https://www.techradar.com/news/what-is-gdpr-everything-you-need-to-know*
[275] *https://www.techradar.com/news/google-fined-pound44m-by-french-data-regulator*
[276] *https://www.oag.ca.gov/privacy/ccpa*

- The right to correct inaccurate personal information that a business has about them.

- The right to limit the use and disclosure of sensitive personal information collected about them.

These rules apply to all for-profit companies that do business in the state of California, even data brokers. There is a carve-out for non-profit entities and somewhat broadly-defined "service providers" that businesses may share data with, such as shipping companies and credit card processors.

As a result of these two pieces of privacy legislation, any company that does business in the EU or California is required to provide users or customers with the ability to request correction or removal of their personal data. Unfortunately most companies force people to prove that they're California or EU residents before accepting these requests; everyone else is excluded. Such is the value of personal data to them.

There is hope at the Federal level, however. As I write this, the American Privacy Rights Act (APRA), which offers many of the same protections as the GPDR and CCPA (without overriding state laws that offer greater privacy protection) and (as of the publication of this book) adds the right of American citizens to individually sue corporations that fail to comply, is being debated in Congress.[277] It was originally proposed in 2022, and has undergone various amendments to achieve bipartisan support.[278] I fervently hope that this bill becomes Federal law by the time you read this sentence (even though it would render parts of this book obsolete), but if not, then I hope you'll contact your Congressional representatives and ask them to support it.

There is a potential risk that the APRA could be further revised or later limited (by Supreme Court ruling) because of the restrictions enumerated in the first amendment of the Constitution, which states that Congress shall pass no law abridging the freedom of speech or the press. However, the Supreme Court has placed limits on free speech in the past, and will likely do so again in the future as culture and technology evolves. The greater concern is with freedom of the press. While the GPDR grants EU citizens the "right to be forgotten" by requesting removal of any content

[277] *https://www.techradar.com/computing/cyber-security/historic-federal-data-privacy-bill-lands-in-us-congress*
[278] *https://www.ft.com/content/1e6587a7-4fb4-449f-8424-29a819b3ae3b*

that contains any of their personal information, the US has historically favored the enshrinement of legitimate news stories as a public record of events that represents "the rough draft of history." However, this precedent was established in an era when an unlimited number of tweets, blog posts, court documents, mugshot photos, and news stories weren't easily found and readily available to the entire world in an instant. I'm optimistic that the US government can find a way to appropriately balance personal privacy in the post-Internet era with traditional first-amendment rights.

Donate to and Support Personal Data Rights

There are some non-profit organizations that have consistently supported privacy and advocated data rights, and are worth your consideration for membership or donation:

- **The Electronic Frontier Foundation (EFF):** https://www.eff.org
- **The Mozilla Foundation:** https://foundation.mozilla.org
- **The American Civil Liberties Union (ACLU):** https://www.aclu.org

Reward the Virtuous, Shun the Wicked

Privacy and data rights should always be considerations when you give money to a business. Certain companies are particularly evil when it comes to hoarding and exploiting personal data; some are habitually careless with information security, and have suffered multiple data breaches; and a few companies are owned by honest people who are just as serious about data rights as you are.

It's worthwhile to read through privacy policies before clicking "I Agree," and to search for a history of privacy violations and data breaches before you purchase an electronic device, car, or Internet service; or sign up for a social media app or subscribe to an online game. Very often the worst offenders are ostensibly the cheapest and most visible in online and traditional media ads. They have to offer various financial incentives and publish influential propaganda because if every customer researched the

market thoroughly, no one would choose them. If there's a data breach at their company, evil executives know that consumers have short memories, so they offer "credit monitoring" or "identity theft protection" services for two years to those potentially affected, and then run a bunch of ads and promotions to pull in a new clutch of deal-seekers and bargain-hunters.

Bad companies can only survive if people don't think before they hand over their money. Likewise good companies can only survive if you put privacy and data rights before cost, convenience, brand loyalty, and propaganda. Whenever you have a choice, reward the virtuous and shun the wicked.

Teach Others Well

You have a great deal of influence over the people you know and interact with. While you can and should encourage others to take reasonable measures to protect their privacy and defend their data rights, words always have less impact than actions. By refusing to surrender your data, or to participate in exploitative social media, or even to let your driver's license be scanned by a liquor store clerk, you not only establish a precedent for others to follow, you also bring awareness to people who have no idea what's happening with their personal information behind the scenes.

As with all forms of advocacy, though, it's important not to be militant, cultish, or judgemental. If your spouse, friend, or co-worker isn't interested in protecting their privacy, then pestering them with unwanted details and criticisms is unlikely to change their minds.

Advocacy can be burdensome; sometimes it's best to refer people to other sources that they can dive into when they have the time. In addition to the resources listed throughout this chapter, I recommend:

- This book, of course! Buy copies and gift them to everyone you know!
- https://whatismyipaddress.com
- https://www.easyprey.com
- https://www.spotthetroll.org
- https://haveibeenpwned.com

The Future of Data Rights

As I write this, the situation seems grim. Personal data is increasingly being collected, created, calculated, sold, and stolen. It's being used to steal money, real estate, and digital assets; to mislead and terrorize people on a massive scale; and to manipulate consumers into wasting time and money for the benefit of huge corporations and the wealthy people who own and manage them. Data breaches, ransomware attacks, and acts of violent vigilantism originating from social media are increasing in number and severity. Professional writers, illustrators, photographers, and actors are fighting to keep their art out of AI data models, and politicians are struggling to combat the effects of deepfake videos and fake news stories about them.

Broadly speaking these ills are not new in concept, they're just much easier, quicker, and more damaging than in previous eras thanks to exponentially-advancing technology. Therefore how you feel about the future of data rights depends on whether you believe there is a hard limit to the potential of computer-based technology. Will there ever be a time when every email, phone call, and text message we receive is wanted, useful, and legitimate? Will AI ever be as capable as a real adult human, without having any human faults or foibles? Will quantum computers be able to break the strongest encryption algorithms? Will security measures ever be infallible to the point that fraud is obsolete?

The *rights* half of *data rights* raises its own set of questions. Will we ever have the power to permanently remove personal and copyright-protected information from all publicly-accessible sources without enabling criminals and despots to erase evidence of their misdeeds? Will we ever be able to have absolute confidence that the articles we read and videos we watch are true, unaltered, and free of subtle influence and propaganda?

Underlying all of these is one fundamental question common to everyone – moral and immoral, selfish and generous, honest and dishonest: Can technology ever be so advanced that it always helps me and never hurts me?

The answer to all of these questions is probably "no." For most of human history we've been trying to make it impossible for people to cause harm to others. Moral codes, economic incentives, methods of punishment, powerful political structures, testing and gatekeeping procedures, and a

vast array of security methods have all promised varying levels of safety while also providing clearly-defined paths for circumventing them. But it is human nature to keep trying; to keep refining and evolving our social, political, and technological systems to close the loopholes and make it more difficult for criminals to steal from us and for corporations to take advantage of us. It will never be impossible for a bad actor to achieve his or her goals, but it will continue to become more risky and costly – and that's the best we can do.

Therefore I believe the future will look a lot like the past: spam filtering will get better, but it will never be perfect; security methods will become harder to defeat at the cost of convenience, usability, and accessibility; scams and fraud will constantly adapt to work around those new methods; and governments will become increasingly involved with combatting the societal problems caused by personal data collection. All the more reason to take to heart what I've communicated in this book; while some details will change over time with new regulations and technologies, the fundamental principles and practices will always apply.

The End