DISENGAGE

ESCAPE THE LEASH OF BIG TECH, SCAMS & SURVEILLANCE

They took your data, your time and your peace.
Time to reclaim what's yours.

BY REX T. FLOOF PUNCHING UP PRESS

DISENGAGE

ESCAPE THE LEASH OF BIG TECH, SCAMS & SURVEILLANCE

Everyday Resistance for the Digital Underdog

By Rex T. Floof

TABLE OF CONTENTS

FOREWORD

ARE WE IN PARADISE YET?

Imagine your town has a public square. It isn't perfect... there are no fancy fountains or ice cream stands, but it's a pleasant place to hang out with your family and friends.

The city sells the square to a few large companies, who rename the area "Paradise Square." They upgrade the bathrooms, add athletic fields, and install the fancy fountain and ice cream stand the place was missing.

Everything is great. The ice cream is so cheap! The toilets in the bathrooms have heated seats!

Then things start to change. The businesses that own the square install retina scanners at the ice cream stand, bathrooms, fountain, and athletic field. Whenever you use one of these amenities, information ranging from your name and address to your physical attributes and income is sent off to some shadowy entity. Not only that, but the ice cream stand starts selling knockoff treats.

You start noticing more and more that something is off. Before you do so much as sit on a bench, you have to sign a waiver that's too long and complicated to actually read through. The company that installed the bench tells the ice cream stand what kind of pants you're wearing, and the ice cream people use that detail to parse out what kind of ice cream you like best so they can hawk it to you the next time you walk by. (Ooh, those Dolce & Gabbana cargo pants must mean you'll spring for extra sprinkles!)

Each time you sign a waiver and sit down, you're beset by dozens of skeezy salespeople who all seem to know your name. Sometimes they're already there when you approach the bench, and there are so many of them you can't even sit down. You even start seeing them outside the park—on billboards lining the highway, at the movie theater, on top of taxicabs.

A few times, your wallet is stolen. You also notice people hiding in the bushes with recording devices. For reasons unknown, they're recording your conversations with your friends.

The ice cream stand goes out of business. The park had required them to charge such low prices, the owner couldn't pay their employees sustainable wages.

Even worse, you have nowhere else to meet your friends and family. Thanks to all the cheap goods and formerly fine amenities, so many citizens flocked to Paradise Park that the other parks quietly closed down.

As you sit on the rigged bench, hungry, mikes in your face, salespeople circling, you ask yourself:

“Is this really Paradise?”

INTRODUCTION

THE POWER WE DIDN'T KNOW WE HAVE

If you're reading this, you're probably intrigued by the idea of disengaging from the companies that have made the internet a worse place to be, but are not really clear on why you'd want to do it…and how to make it happen. Especially if you're already busy, you know, living life.

Read on to learn what inspired me to write this book, discover our secret power, and get some important caveats out of the way before we dive in.

THE ORIGINS OF THIS BOOK

When I started my freelance company in the 1990s, most of my business was conducted via the library and post office. Over time, however, the internet became my go-to for developing ideas, researching prospects, and sending sales letters.

Even this early on, I was uncomfortable with the ubiquity of ads and how they seemed to follow you wherever you went. In 2000, I started a blog—though back then it was called a "weblog"—where I highlighted instances of ads showing up where they shouldn't be: inside the holes on a golf course, on urinal cakes, in schools. The website

garnered some positive attention, but I shuttered it when I became too overwhelmed with paying work to keep it up.

The spirit of the weblog lived on

As an entrepreneur online, I tried so hard to work within the system that had been set up for us. I joined every social platform that popped up, took marketing gurus' advice to heart, and subscribed to the whole "rise and grind" mentality.

But the spirit of my old weblog always lived in me.

- I was an active member of SPAM-L, a listserv of mostly software experts who parsed out the headers of spam emails to report the senders to their Internet Service Providers.
- I went to a conference for online business owners, and felt like a total weirdo when I raised my hand in front of the fawning audience and asked the internet-famous presenter, "You brag about being available to answer questions from clients at 4 am. How is that… scalable?"
- When a business coach I'd hired asked what style of business owner I wanted to be, I answered, "I want to just do good work and have people who need it, buy it. Is that so wrong?"

- I stopped offering mailing list sign-up incentives and chopped my list from 10,000 lurkers to 800 engaged readers. Why pay to reach people who didn't care?

I despised having to keep up with the ever-changing whims of social media, internet marketing rockstars, and Google-pleasing content formats in order to stay afloat. (Micro content! No, long-form content! No, wait...video! Haha, j/k about all those videos you spent loads of resources creating.)

Beyond business, I was tired of finding my personal information where it shouldn't be.

I hated that corporations were privy to intimate details about my family, income, spending habits, hobbies, voting record, and property—which they used to try to sell me solutions to problems I never knew I had. Not to mention, these companies' lax data protection processes meant my private details were compromised in data breach after data breach. (And this is not a problem only for the living: A deceased relative recently had their personal data leaked.)

I resented being forced to buy from megacorps like Amazon because the products I needed were no longer available anywhere else.

I hated the idea that my content, labor, dollars, data, and attention were feeding these companies and helping them grow more powerful.

Finally, I couldn't remember what it felt like to move through the world without a sense of being constantly watched—without worrying, for example, that someone's Alexa will record and share me saying something better left unsaid. Yet I experienced the irresistible pull to be online all day long, feeding the companies that oppressed us, lest I miss the chance to attract attention.

Reclaiming our power

But what could *I* do about it? I started researching and reading about surveillance capitalism, monopolies and monopsonies, chokepoint capitalism, the decline of common spaces, and other relevant topics. It was disheartening to get to the end of a book only to learn that the solutions were always structural...because, of course, structural problems require structural solutions.

I get it. We clearly need to push for better privacy legislation, stronger antitrust laws, and better lobbying laws.

But I didn't read all those books and do all that research because I wanted to learn what *other people* could do

about the problem. I wanted to know what I—a middle-class retiree who doesn't like politics, protesting, or public speaking—could do about it.

Not to mention, it took 40+ years to get us into this mess. Even if we work full-speed ahead to undo it, we will have to live under this system for many years. What can we regular humans do to protect ourselves and others now, before all the right societal changes finally come about?

Here's the great news: Even as digital underdogs, we have power we can wield using the time and resources we have right now. That power is in:

- Our data
- Our content
- Our labor
- Our participation
- Our attention
- Our dollars
- Our permission

These are the lifeblood of the businesses destroying the internet and controlling our lives, and we can all withdraw at least some of them to some extent. We can subvert the system in small ways. We can refuse to be profiled, pigeonholed, pinned down.

We can *disengage*.

This is why, in the spring of 2023, I embarked on an ambitious three-part project: I wanted to drastically reduce the amount of time I spent online, shrink my digital footprint, and reclaim the sources of power I listed above.

The purpose of this guide is to share what I discovered on this journey, in case it might help others the way it's helped me. There are no affiliate links in the guide, and it's free. I don't track who downloads the guide.

If you would like to show your appreciation for *Disengage*, here are three suggestions:

- Share the guide with at least one person.
- Sign up for infrequent, non-spammy updates at punchingUPpress.com.
- Volunteer to distribute postcards for this book, "guerrilla marketing" style. Put them in books at the bookstore, in Little Free Libraries, at the gym, etc. I'll even mail you the postcards! Email me at punchinguppress@proton.me.

In short, if you want to say thanks…the best way is to help get this book into more people's hands!

WHAT'S NEW IN THE 2025 UPDATE

I updated this guide in 2025 for three reasons:

1. After the 2024 election, it seems clear that the very corporations that we're fighting against here will now have almost unlimited power. I expect that surveillance will increase, consumer laws will be weakened, and many of our elected representatives will cave in to the lure of money and power offered by these businesses.

2. Artificial Intelligence has been scooping up more and more of the content we've spent so many years diligently creating online.

   In some cases, it's to spit out that content in a "new" form, such as when an AI uses real content creators' work as fodder to create fast and free content, whether written content, video, or art...cutting the actual content producers out of the picture. (A big drive behind AI is to "train" it using employees' and vendors' work so it can later replace those people in their jobs.)

   In other cases, AI's purpose is to invade our privacy by, say, using online photos to learn how to identify people.

3. Businesses and institutions are now trying to use our demographic and behavioral metrics to pull more money out of our wallets, aka "surveillance pricing."

For example, the McDonald's app can tell when you get paid and increase the price of your order that day. Some car brands share your driving data with your auto insurance company so the company can raise your rates if they think you take corners too fast. Grocery stores are experimenting with personalized pricing based on your data, meaning that bag of apples may cost more for you than for your neighbor.

Here are some of the changes I made to Disengage.

- Updated links, prices, and advice. New services, social media sites, risks, and possibilities for disengaging have come into being since the original writing, and I wanted to be as thorough as possible.
- Added a chapter on corporate-controlled news media.
- Added ideas that are a bit more tech-heavy to match the seriousness of the situation we may be facing in 2025 and beyond. If you're not a technophile, simply skip these tips.
- Made changes to reflect what I've learned in the past two years of implementing the advice in this guide; for example, I added my experiences with using a "dumb phone," trying out a paid search engine, installing a privacy OS on my phone, and using a PO box. Some of these were wins, and some were fails.

The world changes fast! I hope this updated version of *Disengage* helps you reclaim your data, dollars, labor, and attention...and in doing so, helps reshape the country to reflect the needs of regular people instead of billionaires.

WHAT YOU'LL LEARN IN THIS GUIDE

Disengage offers my research, experiences, and advice in the following areas.

PART 1: Why Disengage?

Here, I quickly discuss the concepts of surveillance capitalism, chokepoint capitalism, the exploitation of our common spaces, and the billionaire ruling class, aka the "broligarchy." You'll also discover the side benefits to disengaging, and get a reality check on how much of our power we can reasonably reclaim.

PART 2: Disengage By...Reclaiming Your Data

We'll tackle how to control your online accounts, secure your phone and email, remove unwanted photos and personal information from the internet, remove your details from data broker lists, and much more.

PART 3: Disengage By...Reclaiming Your Home

You'll keep our corporate overlords—and other randos—from peeking into your home by hiding your home

address, removing photos of your home from real estate sites and street view apps, and keeping smart home products from tracking and sharing your private data.

PART 4: Disengage By...Reclaiming Your Content

Your unpaid content is the very backbone of the businesses that are oppressing us. You'll learn how to rein in content you've already posted, how to quit social media, and how to make your content labor work for you...plus how to shrink your footprint on social media if you don't want to (or can't) quit.

PART 5: Disengage By...Reclaiming Your Attention

All day long, we're pulled in different directions by the whims of the hyper-capitalist companies that have taken over our lives. This section will share advice on how to annihilate ads as well as ideas for ditching the most distracting gadget ever created: your smartphone.

PART 6: Disengage By...Quitting The Big 4

Hopefully, all of the above prepared you for the biggest challenge: kicking Google, Amazon, Apple, and Microsoft to the curb. This section includes alternatives for the most popular products provided by these companies.

PART 7: Live Your Life

They say living well is the best revenge. Here, I offer encouragement as you continue your journey, more ideas on topics to pursue, and appreciation that you took the time to read—and hopefully take action on—this book.

WORKSHEETS

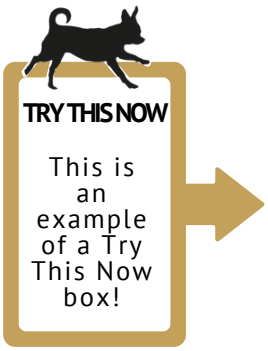
Download these PDF worksheets that help you take action on each part of this book.

WHAT'S IN THE BOX?

You'll find three types of boxes in this guide. And because we're PUP: Punching Up Press, they will be Chihuahua-related.

EXTRA CREDIT boxes are for readers who are tech-savvy and/or like to go the extra mile.

BEWARE boxes include scams to watch out for or caveats to the advice given.



TRY THIS NOW boxes highlight tasks you can do right as you're reading this guide. They're typically quick and easy, or a small part of a larger task that will help get you rolling. You don't *have* to do the Try This Now task right now, even though the Chihuahua is in a hurry. It's your choice.

THE REQUISITE DISCLAIMERS

I did my best to cover as much ground as I could, but I can't possibly include every single detail I uncovered in my research. For example, Google tracks us in so many ways it would take another book to describe them.

Why are you dissing my local grocery store?

You'll notice that the content in this guide ranges beyond the internet at times. Why am I covering direct mail, smart products, and store loyalty programs?

It's because we're attempting to choke off the flow of data traveling from online to offline and vice versa. The less of your personal data *of any kind* flying around the world, the less there is to fall into the hands of those who would abuse it.

How technical is this going to get?

I consider myself a "medium techie" person; I've been on the internet since the early 1990s, and built my first website in 1997 using an HTML guide I found in a phone booth. Having run a business that required me to be online most of the time, I've picked up strong skills in some areas. I even learned enough Python to hand-code a Reddit bot!

At the same time, I don't want to have to get a Ph.D. to minimize my online footprint, increase my privacy, and subvert Big Tech and other oppressors. So I generally use—and recommend—solutions that don't require a lot of technical knowledge.

If I happen to know about, or have used, a more advanced solution for some of the issues in this guide—like syndicating your website content to social media, installing a privacy-forward operating system on your phone, or using emulators to play video games—I'll mention them and offer outside resources where appropriate. If you're interested in any of these tactics, please look up how to implement them.

A note on privilege

I'm in the very fortunate position of having the time to spend plugging away at this endeavor, and available cash for products and services—within reason—to take care of some of the related tasks for me. I also have no disabilities or medical situations requiring me to buy from Big Tech, and don't belong to a marginalized group that can find support only in online communities.

As you'll see throughout this guide, it's easy to adjust this process as needed to make it work for your particular situation. For example:

- Almost all of the products I recommend are free or have free alternatives.
- You decide how much time and effort you want to put into this project.
- You choose whichever tactics make the most sense for you.
- It's up to you how strict or lenient you want to be in various areas to account for your job, schooling, family situation, medical and financial needs, and so on.

Even a small amount of effort can make a difference; for example, installing a free anti-tracker extension, changing your phone settings, getting a "burner" email address, or switching your book buying from Amazon to independent online booksellers will offer some benefit with little time and money spent.

Best of all, most of the effort required is front-loaded. Once you get your chosen systems set up, they should run as smoothly for you as your old ones. (Or even more smoothly!)

For example, it takes a good amount of thought and effort to switch from Apple Music to SoundCloud, or to change your default browser and search engine—but once you do it, you won't have to think about it again.

If you need more help

If you need to protect yourself from a stalker, are being doxed, or otherwise need stronger methods than you'll find in this guide, I highly recommend the book *Extreme Privacy: What It Takes to Disappear* by Michael Bazzell.

I finally bit the bullet and dropped $40 for the PDF version because I was curious...and now I wish I had paid for the hard copy edition. This book is fascinating and very, very thorough. It's a must-read for people who actually need to live under the radar.

In the first edition of *Disengage*, I talked a bit about throwing chaos into corporations' tracking systems as a form of resistance. *Extreme Privacy* goes deep into using disinformation to throw Big Tech off your trail and gave me tons of new ideas, some of which I've already started putting into practice. I'll share some of my experiences, but without giving away so much that it infringes on Bazzell's great work.

If you want to know more, buy his book. It's worth every cent! (Sadly, the author has stopped writing books because so many people downloaded illegal free copies of *Extreme Privacy*.)

PART 1

WHY DISENGAGE?

The biggest threats we're fighting against in this guide are surveillance capitalism, chokepoint capitalism, the exploitation of our common spaces, and the rise of the "broligarchy"; you may have also heard of concepts like Big Data, Big Tech, and the attention economy, all of which play a role here. After reading about these systems, you may decide that you no longer want to participate in them.

CHAPTER 1

WHAT WE'RE FIGHTING AGAINST

Much of the villainy we're going to discuss is perpetrated by just a handful of massive companies, including Google, Facebook, and Amazon. While I will give a brief overview of the ills created by each corporation later in this book, I won't get into lengthy critiques of them since the resources I cite have already done it so thoroughly.

SURVEILLANCE CAPITALISM IN UNDER 200 WORDS

Here's how Shoshana Zuboff, author of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, describes surveillance capitalism in the Harvard Gazette:

> [It's the] unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets—business customers with a commercial interest in knowing what we will do now, soon, and later.

In other words, businesses track us and collect our data in order to build psychological profiles they can use to predict what we'll do or think...so they can sell us stuff we didn't know we needed.

Zuboff points out that surveillance capitalism is like a one-way mirror: The companies know everything about us, yet we're not privy to how they collect, use, share, and sell our personal information.

CHOKEPOINT CAPITALISM IN UNDER 200 WORDS

To put it simply, chokepoint capitalism is when a business inserts itself between buyers and producers, extracting money without adding any value like a troll under a bridge.

Consider Apple: They not only control which apps you're allowed to install on a phone you bought and own, they also claim a hefty portion of the fees you pay to the app producers.

Or Amazon: You buy their e-reader, but can only use it to read e-books you purchase from Amazon. Once you do that, you're locked in; the price of switching to another e-reader is high, because your entire library of books is now held hostage on your Kindle.

This is a very simplified description. The history and methods of chokepoint capitalism are fascinating, including how businesses buy up competitors, and even parts of their own supply chain, to create inescapable monopolies that affect smaller businesses, workers, and creators. I highly recommend reading *Chokepoint Capitalism* by Rebecca Giblin and Cory Doctorow, and subscribing to Doctorow's ad-free newsletter.

THE EXPLOITATION OF OUR COMMON SPACES IN UNDER 200 WORDS

The hyper-capitalist businesses we're resisting here also exploit the places we go to socialize and connect. In other words, they've created a monopoly over how we fulfill some of our most basic human needs.

So many of our friends and loved ones are on Facebook, for example, to leave it means we may have to sever some of those relationships. This is by design. We're forced to check in frequently, conduct our conversations on the platform, and share our news there—giving Facebook more and more of our most intimate data.

THE TAKEOVER BY THE BILLIONAIRE CLASS IN UNDER 200 WORDS

Whatever you may think of the President, the fact that the top tech moguls were front and center at his inauguration is bad news for all of us. According to an article in The Hill:

> [A] growing class of malignant oligarchs has initiated a campaign to exert unchallenged control over our democratic institutions and our economy. The war has already started, and the billionaires have a significant head start.
>
> These individuals are hoarding unfathomably large amounts of wealth and are now wielding it to suppress

critical media, co-opt our politics and defang our justice system. They have rigged our tax system so that they pay dramatically lower tax effective rates compared to working people. They have consolidated corporate power to shield themselves from scrutiny.

A large portion of these billionaires own the social media, tech, and news channels that follow our every move and shape our reality. They live on attention and suck up our labor and data to grow their power.

Surveillance capitalism, chokepoint capitalism, the exploitation of our personal spaces and relationships, the threat of “broligarchy” in 2025: *We* are nurturing the businesses to blame for these societal ills by constantly feeding them everything they need to thrive.

CHAPTER 2

HOW DO WE RECLAIM OUR LIVES BY DISENGAGING?

When we disengage, we take everything with us: our data, our content, our attention, our money. Without all this, the exploitative businesses that have taken over can't survive.

In other words, when bigger players are pushing you around the court, you take your ball and leave. You go off and play with nicer people, and the bullies are left with nothing.

THE SIDE BENEFITS TO DISENGAGING

Maybe it's wishful thinking to believe we can do enough damage to take down the tech oligarchs who are invading our lives and damaging our communities. But even if we lose this battle, we can still win the war by claiming some important side benefits.

Side Benefit #1: We protect ourselves against identity theft

The more places storing your data, the more opportunities there are for that data to fall into the wrong hands. It seems like every month or so, I get an

email from some company I did business with a decade ago letting me know their databases were breached, exposing my personal information to bad actors.

Cory Doctorow writes in Medium:

> Like spies, online fraudsters are totally dependent on companies over-collecting and over-retaining our data. Multiple services have suffered breaches that exposed names, addresses, phone numbers, passwords, sexual tastes, school grades, work performance, brushes with the criminal justice system, family details, genetic information, fingerprints and other biometrics, reading habits, search histories, literary tastes, pseudonymous identities, and other sensitive information. Attackers can merge data from these different breaches to build up extremely detailed dossiers on random subjects and then use different parts of the data for different criminal purposes.

So it makes sense that the less data of yours that's available, the less likely criminals will be able to use it against you. (Not to mention, it will make it harder for surveillors to profile you, harder for businesses to use your behavioral data to swindle you, etc.)

Side Benefit #2: We become harder to find

As I mentioned earlier, this guide isn't meant to help readers evade stalkers or protect themselves from doxers or targeted surveillance.

However, making yourself harder to find online can help dissuade bad guys from targeting you. Someone who's mildly pissed off at you, for example, may not bother to send you anonymous threats if it takes too much effort to find your phone number, email address, or home address.

Side Benefit #3: We protect our mental health

We've all seen the news about how social media contributes to anxiety and depression, how being online too much can affect our sleep, and how email, texting, smartphones, and social media are designed to be as addictive as possible. The sounds, the colors, the three dots when someone is typing out a reply to our text, the satisfying little vibration when we successfully download an app…how can we *not* remain glued to our devices?

Then there's our tendency to think social media represents the real world, and to compare ourselves to what we see in highly staged posts. (Which is by design.)

We see photos of a well-groomed mom with a perfectly dressed baby and wonder what's wrong with us that our lives don't look like that. We see images of family on an exotic beach and feel like a failure because the nicest place we've ever visited is the Holiday Inn in Newark. We watch a video by a fitness influencer who tells us he looks the way he does because he drinks Brand X protein shakes, and feel like losers because we don't have the strength of will to follow his "simple health plan."

What we *don't* see;

- The pile of dirty clothes the mom shoved into a corner before the shoot.
- The three hours she spent on her hair and makeup.
- The baby's diaper blow-out ten minutes earlier.
- The family fights on the sweaty vacation.
- The hefty check the family received from the sponsors of the vacation you could never afford.
- The way the fitness influencer straight-up lies about his eating habits because he's sponsored by the protein shake company...and also that he takes massive amounts of steroids to look the way he does.

None of this is good for us. That's why, for some of us, disengaging can be an exercise in protecting our own mental health.

Side Benefit #4: We do better work

Our jobs, businesses, and schooling are important to us, and the internet is making these things harder—not easier as we were once promised—because it puts a crimp in our ability to focus and be creative.

According to a Microsoft survey:

> We're all carrying digital debt: the inflow of data, emails, meetings, and notifications has outpaced humans' ability to process it all. And the pace of work is only intensifying. Everything feels important, so we spend our workdays trying to get out of the red. Nearly 2 in 3 people (64%) say they struggle with having the time and energy to do their job—and those people are 3.5x more likely to also struggle with innovation and strategic thinking.

Of course, those of us who are in careers, businesses, or school aren't in a position to simply drop Big Tech and all its products. But we can scale back enough to regain the crucial life and business skills we've lost.

Side Benefit #5: We live our lives through our own eyes

So much of online life is about seeking validation from others. After all, is there anyone alive who posts their thoughts, images, or personal details on the internet and *doesn't* care about how many likes or comments they get?

This causes us to live life through the lens of a camera—even if it's only a mental camera. When I was full-on bound by social media, no matter what I did, I would unconsciously start to put together a post about it in my mind. How would I make this thought sound more insightful? What hashtags would I use? What would be the best way to frame the image?

Once I scaled back, I started being able to enjoy my life for myself. I can now watch a sporting event, see a movie, read a book, or go on vacation without feeling the need to share it with the world. I can have a brilliant idea or laugh at a joke I heard and keep it to myself.

If I have a thought I really, really want to share, I can put it up on my own website and trust that if anyone is interested, they'll find it.

Side Benefit #6: We rebuild our decision-making skills

Sometimes we rely on the hive mind of the internet so much, we forget what we want. There was a period of time when my first instinct, when I couldn't figure something out, was to head to a forum or social media to ask for input. Do the colors in this drawing make sense? Would it be stupid to pay off a debt faster instead of investing the money? Are these jeans age-appropriate? The alternative was to ask Google...and get answers from a company with a stake in the answer.

I got answers aplenty, no thought required on my part. But were the choices really mine when I crowdsourced them?

The system was built this way. A voice search expert once told me that businesses were noticing that many searches started with "Should I...?"

The expert was giddy about the idea of people turning to faceless corporations to help make life-altering decisions—and offered up ways to make a brand appear trustworthy and knowledgeable by providing voice-search answers to these personal questions. (Should I buy a new pool? Why, yes, says the pool company, and here's why! Should I feed my cat dry kibble? No way, according to the "primal" raw cat food company.)

When I started to disengage, I had to start relying on my own instincts, tastes, and preferences. Which is actually a good thing, because these are my possessions, my money, my clothing. I'm allowed to do whatever I want. I can draw in whatever colors are pleasing to my eye because I'm hanging the drawings in my own house. I can invest my money in whatever way makes sense to me, even if it's not approved by a bank or investment firm with a stake in my decision.

Now if I have a question or problem, I research it on my own, take my own preferences into account, and make up my own mind.

Did you know you can do that? I didn't, because the internet makes it so easy to ask for advice and validation that my decision-making muscles had withered into nothingness.

Opting out—to whatever extent you want to do it—helps you relearn your own likes, dislikes, needs, and wants and gives you the power to make decisions that work for *you*.

Side Benefit #7: We stop supplying free labor to for-profit businesses

You may not know it, but you are a content producer. Everything you post online is used by social media companies, app developers, publishers, travel agencies, supplement sellers, and other businesses to gain legitimacy—and, ultimately, more eyeballs on whatever it is they're trying to sell.

They also use that very content to gather data from you and from everyone who engages with it. (To add insult to injury, some businesses are using that content to train AI.)

When you post an inflammatory remark on Twitter/X, the firestorm of outrage benefits the platform and its advertisers while impoverishing you and your community. The comment you post on a news story brings more readers to the page, partly because Google's search algorithm rewards pages with more content and more frequent updates.

These businesses need your content in order to survive and grow...and you don't even get paid for it. Let's stop spending our precious life energy keeping our oppressors in business!

In Chapter 16: Say Sayonara To Social Media, we'll talk about alternative homes for content for those of us who make a living by building audiences or selling products and services online.

Side Benefit #8: We save money

It's true! Even if you choose to purchase tools to help you disengage, you'll make up for whatever you spend because you will:

- Learn to think about a purchase before running to Amazon the instant you decide you need something.
- Free yourself of your Amazon Prime subscription, encouraging you to look for lower prices elsewhere. (As you'll learn later in this guide, Amazon does *not* prioritize good deals.)
- Purchase cheaper alternatives to overpriced devices.
- See fewer ads enticing you to shop, shop, shop.
- Earn more in your business because you aren't spending your time on ineffective social media marketing.
- Buy fewer apps and make fewer in-app purchases.

- Turn to free, open source software in place of some of your subscription-based software.
- Stop losing money to branded apps that use surveillance pricing to charge you as much as they determine you can afford.

What will you do with all the money you save by disengaging?

Side Benefit #9: We inspire others…and ourselves

When you make choices that are different from what most others are doing, it stands out. People will ask you about it.

For example, when I experimented with using a non-smart phone, even my optometrist was curious to know more. This gave me the opportunity to say, “I felt like I was getting addicted to my iPhone. So I switched to a non-smart phone as an experiment, and feel like my attention has improved. I don’t even miss it anymore.”

People usually respond by sharing their own experiences with divided attention, constant interruptions, and feeling tracked. Maybe some of them will wind up, if not ditching their smartphone altogether, at least deleting the most distracting apps or turning on the privacy controls.

So when someone asks you about your strange-looking email address or why you don't shop on Amazon, it's an opportunity to—quickly, non-judgmentally, and non-pedantically—explain your choice and hope it gets them to think differently.

On top of that, every action you take to withdraw your attention, data, content, and dollars from Big Tech requires a little effort, which strengthens your will to take even bigger actions in the future.

CHAPTER 3

GIANTS IN THE DARK

Maybe you want to scale back a little—or maybe you want to break up with our corporate masters and never look back. Consider this guide an idea book; it's a list of strategies to pick and choose from depending on your wants, needs, resources, and abilities.

However, we first need to consider the forces working against our desire to disengage.

FORCE #1: THE ENEMY IS OVERPOWERED

A lot of very smart people are working very hard to gather our data, make sense of it, and use it for their own gain. They're deploying powerful software and using every tech tool at their disposal to make this happen… while we're too busy working, caring for our families, and generally living our lives to resist with the same intensity.

These businesses have taken over the internet in a way that makes them hard to evade. "Amazon, Google, and Meta (formerly Facebook) have become pillars of the modern internet infrastructure, and are impossible to completely avoid," reports PCMag. "Even if you deleted all your accounts and never used them again, they'd still probably be able to harvest data on you."

These same companies have engineered their products to become essential tools for connecting with other people. They then exploit our personal relationships to encourage us to share, like, post, and comment—in other words, to generate content that produces more and more data about us they can capture and use in a never-ending cycle. Meanwhile, they work to make their products as addictive as possible, literally using the science of addiction to keep us glued to our screens so they can keep pumping us for data.

Data capitalists then combine the data they harvest directly with data they get from third parties to form a complete profile of us as individuals. And we can't stop it! Just check out this gem of a privacy policy clause from—of all things—a school yearbook company.

> Please note that we may combine information that we collect from you and about you (including automatically-collected information) with information we obtain about you from our affiliates and/or non-affiliated third parties, and use such combined information in accordance with this Policy.

Dare to so much as buy a yearbook and you become part of the bonanza of data the corporate oppressors use to track and try to control us.

FORCE #2: WE HAVE TO USE THE INTERNET FOR ROUTINE TASKS

It's now nearly impossible to do banking, buy concert tickets, plan a trip, pay bills, or take care of many other common tasks without going online.

FORCE #3: EVEN WHEN WE'RE OFFLINE, WE'RE ONLINE

Surveillance capitalists don't track you only when you're sitting at your laptop or scrolling on your phone. When you buy running shoes from an athletic store, for example, the transaction—including what you bought, how you paid, and your demographic details—ends up in a database somewhere in the cloud. When you visit your doctor, the details of the appointment are, you guessed it, logged into an online database.

FORCE #4: IT'S LIKE TRYING TO HOLD BACK THE TIDE

Even if you were to wipe the slate clean, it would fill up again before you managed to shut your laptop.

For example, say you somehow manage to magically reclaim every drop of your data…and then your kid joins a sports team. The team requires parents to communicate via an app, upload medical forms to a portal, and use yet another platform to volunteer at the concessions stand. Suddenly, three more businesses have your info, along with the third-party services they share your details with.

FORCE #5: WE NEVER KNOW IF OUR EFFORTS ARE WORKING

One of the hallmarks of surveillance capitalism is that the businesses know what data they're collecting from us, who they're sharing it with, and how they're using it—but we are kept in the dark.

This means you might, say, ask YouTube to stop tracking your viewing history, and they'll say they've stopped. But you'll never really know if it's true, or what other types of tracking they may be doing that you don't have control over.

For example, in 2023, Gizmodo reported that Apple was harvesting data about its users even after they selected the iPhone privacy setting to "disable the sharing of device analytics altogether." Apple later admitted they collected anonymized data for advertising purposes, which has resulted in at least a dozen class-action lawsuits against the company.

FORCE #6: MANY OF US MAKE A LIVING BY BEING VISIBLE

Finally, if you're a public figure or business owner of any kind, you'll probably never be able to disengage altogether. Whether you're a member of the school board, a bakery owner, or a stand-up comedian, details about you will appear on review sites, booking sites, order sites, and even your state business authority's website… at least if you want to keep your job.

In other words, it's difficult to stay offline if your livelihood depends on your being visible online. I spent over two decades as an entrepreneur. I marketed on social media, did interviews with the press, joined business groups online, was a guest on podcasts, and even had my face and name on a screen in Times Square. I can never get all the toothpaste back in the tube now that I want to scale back.

All that said, disengaging as much as we can is still a worthwhile endeavor. Small efforts, when compounded by thousands or millions of people, add up—and we reap personal benefits by reclaiming the life energy the broligarchy has taken from us.

PART 2

DISENGAGE BY...RECLAIMING YOUR DATA

Our data is one of the most nourishing possible substances for Big Tech and the broligarchy that runs it. Everything we do, everywhere we go, our spending, income, grades, sexual preferences, medical information—our lives are there to be consumed, chewed up, and spit out for commercial profit.

I have a friend who vigilantly protected their data from the first moment they went online decades ago. Their name appears in only two places on the entire internet, and those instances are obscured by the hundreds of other people who share my friend's name (and who weren't as careful with their data).

Sadly, I doubt any of us can manage this feat if we're starting from scratch right now. But there are still ways to reclaim some of our data from the invasive, exploitative companies that are using it to thrive and grow.

CHAPTER 4

PAY ATTENTION TO PRIVACY POLICIES

How likely are you to wade through pages and pages of a privacy notice before clicking Accept? “Only about one-in-five adults overall say they always (9%) or often (13%) read a company’s privacy policy before agreeing to it,” according to Pew Research. “Some 38% of all adults maintain they sometimes read such policies, but 36% say they never read a company’s privacy policy before agreeing to it.”

This makes sense, considering how many privacy policies we’re asked to sign, how long and confusing they are, and how they often bind you to the privacy policies of third parties—which you’re also expected to read!

You’ll just have to accept the terms anyway if you want to access the content or website or service…so why bother?

To be totally transparent, I tried reading every privacy policy over the course of a year or so, and found it to be too much effort for the payoff.

Despite this, making a habit of at least skimming privacy policies can be worthwhile. Those policies inform you of

your rights, which you can then exercise; for example, an app's privacy policy may tell you how to opt out of sharing your data with third parties, or give you an email address to write to in order to request data deletion.

If a company's privacy policy is way out of line, voice your concerns to the responsible party; many policies offer an email for correspondence. The more of us who speak up, the more likely it will make a difference.

CHAPTER 5

CONTROL YOUR ONLINE ACCOUNTS

This part can be fairly time consuming, but it's also easy to do bit by bit during spare moments of time. Waiting for a Zoom meeting to start? Sitting in a waiting room? Bored during an intermission? These are perfect times to chip away at the project.

I started by creating a spreadsheet where I logged every business I could think of that might have my data—from stores and apps to utility companies and credit card providers.

Download my Excel template for free to use on your computer or upload to a cloud-based spreadsheet platform. You'll find separate tabbed sheets for accounts, people-search sites and data brokers, bios, and reviews; there's more on all these later in the book. I pre-populated the sheets with common examples, including over 80 people-search sites and brokers. Hover over cells that are marked with a triangle in the corner for explanations/instructions.

A good way to ferret out all the companies storing and sharing your personal data is to look through whatever platform you use for storing your passwords, such as Google Password Manager. This surfaced an incredible number of accounts I had forgotten all about.

Be sure to also check your bank and credit card transactions to dig up businesses that have your info; for example, you may be reminded that you have a Chewy subscription for your pet's food, or notice that your state's toll authority charged you to refill your car's toll pass.

When you're brainstorming the list of all the places your data may be stored, also consider:

- The apps on your phone and other devices
- Newsletters you've signed up for
- Long-forgotten email addresses at Yahoo, Hotmail, etc.
- Loyalty programs you belong to
- Online forums you participate in
- Your credit cards
- Banks where you hold accounts
- All the apps on your TV, such as Netflix or AppleTV
- Social media sites like YouTube, Facebook, and TikTok

- Work-related apps and websites like Slack, Zoom, and Trello
- Smart TVs, refrigerators, cameras, doorbells, thermostats, door locks, cars, etc.
- Utilities and services like the gas company and your internet provider
- Brick-and-mortar shops you frequent: grocery stores, big-box stores, local shops, and so on

Once you have a list, decide which subscriptions/accounts/etc. you want to delete, change, or protect. (Before tackling your social media and smart home products, though, be sure to read Chapter 16: Say Sayonara To Social Media and Chapter 13: Banish Smart Products From Your Spaces to determine whether you'd prefer to get rid of them altogether.)

Where should you start? The easiest place to begin is with accounts you no longer use. For example, maybe you signed up for a website to get a 10% discount on a single purchase three years ago, and you don't plan to shop there again. (Or you decide you'll make future purchases using a guest account instead.) These accounts are prime candidates for closing.

STEP 1: REQUEST DATA DELETION

Before closing an account altogether, check out the site's privacy policy to find out whether and how you can request that your data be deleted. Not all businesses will

erase your data when you close your account! If that's the case, even though they won't be able to collect first-party data on you in the future, they'll still retain your information in their database.

If an account allows for data deletion, follow the instructions in their privacy policy to do so.

STEP 2: IF THAT DOESN'T WORK, POISON YOUR DATA

Some businesses will refuse to delete your data if you don't live in a state or country with consumer privacy protection laws in place. In those cases, log in, delete whatever details are not required, and then randomize the rest of the data—for example, putting in a fake name, throwaway email address, and burner phone number.

Then change your password to a long, random string of characters, log out, and be done with it. Doing this won't erase details on your past activities, but it may be the best solution in this situation.

STEP 3: CLOSE THE ACCOUNT

Once your data is deleted (or poisoned), close the account. If the company makes it difficult to figure out how to do so, look up "how to delete [company name] account." Often you'll find instructional articles or videos created by people who have figured it out.

STEP 4: CHANGE YOUR NAME

I'm not telling you to legally change your name, but to choose a pseudonym for accounts you want to keep open that don't really need to know your name. Think of a name that's close enough to your real one that mail addressed to it arrives in your mailbox without any problems.

For example, if your name is Alexander McAndrews, try Lex Andrews. Tonya Jamison may become Tony Jameson. Or if you are married and kept your maiden name, use your spouse's last name instead...especially if their last name is more common than yours.

The hope is that over time, more data will be attached to the fake name than the real one. Alexander McAndrews doesn't read gardening content, search for eczema cures on Google, and belong to a coffee-of-the-month club... Lex Andrews does!

At the very least, this tactic will throw a bit of sand into surveillance capitalists' gears.

CHAPTER 6

BASH THE BROKERS

When I say your data is for sale, it's not a metaphor. I mean it literally. According to the Electronic Privacy Information Center:

> Thousands of data brokers in the United States buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. As the data broker industry proliferates, companies have enormous financial incentives to collect consumers' personal data, while data brokers have little financial incentive to protect consumer data.

Thankfully, many broker databases let you remove your data—and once you put some of the other suggestions from this guide into action, the brokers will have less and less of your information to collect and sell.

BASH THE BROKERS BY...REMOVING YOUR INFO FROM PEOPLE-SEARCH SITES

You search for an old friend online and see ads promising to show you their address, income, and criminal record. These are called "people-finder" or "people-search" sites, and they scrape and share your data for profit—including your property history, voting records, age, job history, contact info, and relatives' names.

While these sites let you opt out, the bad news is that you need to stay on top of it because over time they'll rescrape and repost your data. Thankfully, the more you delete and conceal your info online, the less the people-finder sites will have to post.

DIY the deletion

A friend of mine made a project of opting out of a handful of people-finder sites at a time; when she's done with the list, she circles back to the top and starts over. This is a good way to approach this task without spending a dime.

Yael Grauer seconds the DIY idea in a report she co-wrote for Consumer Reports called "Data Defense: Evaluating People-Search Site Removal Services." The report notes that even the most effective paid service is less effective than manually opting out of these sites.

If you decide to go the DIY route, keep in mind that some people-search sites require you to be a paid subscriber to access your profile...which you need to do in order to opt out. In these few cases, I use a masked credit card to sign up for a trial or pay for a monthly subscription, then cancel right away. (Even if the site attempts to keep charging me, it can't because I only loaded the card with enough money for one month.)

Other sites ask you to upload your ID. Use ThisPersonDoesNotExist to generate a fake headshot to cover your real photo; IntelTechniques reports that most sites don't examine the photo.

Make it easier by tackling the top ten

According to IntelTechniques, many smaller people-search companies get their data from:

- Spokeo [opt out here]
- Mylife [opt out here]
- Radaris [opt out here]
- Whitepages [opt out here]
- Intelius [opt out here]
- BeenVerified [opt out here]
- Infotracer [opt out here]
- TruePeopleSearch [opt out here]

Also included in this list are LexisNexis and Acxiom, which I address below.

If you start with this group and wait a week or so, you may find that your personal info has disappeared from some of the smaller sites as well.

Trade money for time

If you're low on time and have some cash to throw at the problem, services like DeleteMe (which I have used and liked) will handle this for you on a quarterly basis and

send you reports with the results. DeleteMe costs $129 per year, with discounts for more people and additional years, and targets over 50 top data broker sites. The service will also handle one-off requests if you find your info on a site they don't normally tackle.

DeleteMe also offers masked emails, credit cards, and phone numbers (more on those later).

Here are similar services to check out:

- Incogni costs $89.88 per year and promises to remove your data from over 200 sites.
- Reputation Defender provides additional reputation services such as correcting inaccurate search engine results. They ask potential customers to call them for a personalized price quote, which makes me think they're probably pretty pricy.
- EasyOptOuts is only $19.99 per year and claims to opt you out of over 160 sites.
- Privacy Pros offers a service for $299.99 per year that removes your info from over 300 sites and then asks Google to remove your profile links as they're taken down. (Or DIY that last part! See Chapter 7: Surf In Secret for a how-to.)

There are several other services providing pretty much the same thing; just search for "data broker opt-out services." Even if you don't want to use one of these,

many of them offer free guides and other resources for DIYers.

Keep in mind that these services don't catch every single people-finder site—there are a lot of them, and they tend to multiply and merge—so I supplemented DeleteMe's efforts by opting out manually from additional sites I found on Yael Grauer's incredible list, which includes opt-out instructions for each site. Michael Bazzell's book *Extreme Privacy* also includes a long, long list of these sites, and there's a good list of opt-out links on Arul Selvan's Selvan Soft Blog.

You may hear about the people-finder opt-out service OneRep. In March 2024, it was discovered that the CEO of OneRep also founded dozens of people-search firms—meaning they are potentially selling your info on one end and then charging you to remove it on the other. I recommend avoiding OneRep, especially since there are so many other services out there.

BASH THE BROKERS BY...BEGINNING WITH THE BADDEST

The people-search sites look piddly when compared with gigantic data brokers that specialize in compiling and

selling your data. These businesses collect and share information on everything from your income and purchasing habits to your school grades and date of birth.

Why does size matter? Because the bigger the databases, the bigger the breach. For example, in 2018, it was discovered that Exactis—a now-defunct data warehouse of more than 3.5 billion records used by digital marketers—had 340 million records sitting on a publicly accessible server.

So it's important to opt out of these companies' databases not only because they sell your private information far and wide, but because they can expose tons of your personal data.

Some of the paid opt-out services we talked about earlier remove your info from large data brokers as well as people-finder sites. But if yours doesn't, or if you don't want to pay at all, it's easy to hit the biggest brokers yourself. Keep in mind, however, that a broker may refuse to delete your info if you're not in a state or country with consumer privacy protection laws in place; if this happens you may need to try something else, such as asking them to not share your info.

Here's how to opt out of the most massive data brokers. Be sure to opt out your family members as well!

How to opt out of Acxiom

Acxiom is a data collection and audience identification company that provides marketers everything from your relationship status to your purchase habits.

Opt out, request data deletion, or request access to your data by filling out this form.

How to opt out of Epsilon

Epsilon is a data-driven marketing company. In 2011, hackers stole 250 million records from 75 of Epsilon's clients.

Exercise your privacy rights with Epsilon by filling out this form or (in the U.S.) calling 866-267-3861.

How to opt out of Oracle

As of September 30, 2024, Oracle is no longer in business. If you have any questions, contact oracleadvertising-inquiries_mb@oracle.com.

How to opt out of LexisNexis

LexisNexis collects billions of records, including data from 1.5 billion bankruptcy records.

Opt out of LexisNexis by filling out this form. You will receive an email or postal mailing (your choice) with additional information or instructions.

How to opt out of Nielsen

Nielsen provides survey-based data from more than 90 million households.

Opt out of Nielsen by entering your email address into this form. If they have any information associated with the email, they'll delete all the data from their records. Enter every email address you have just to be sure all your data is deleted.

How to opt out of CoreLogic

CoreLogic provides financial, property, and consumer information, analytics, and business intelligence.

To opt out, send an email to privacy@corelogic.com. They don't provide any info on what to email them, so be sure to include your name, email, and address, and request they delete your data and cease sharing your information with third parties. (It sounds like they may not comply with deletion if you aren't in a protected state, but it doesn't hurt to ask.)

How to opt out of Foursquare

Foursquare helps marketers target customers using real-time location data—meaning, in short, they use technology that can track your phone so marketers can push ads to your device whenever you're near their location.

To opt out of Foursquare, the company requires you to enter your iPhone's iOS Advertising Identifier (IDFA) or Android phone's Android Advertising Identifier into this form.

For Android users, the process is simple: To find your Android ID, just open up the Google Settings app and go to Ads. Your ID should be visible at the bottom of the Ads page.

An Apple user? As of iOS 14, you have no way to access your IDFA without using a third-party app. If you want to take a chance, here's a list of IDFA-revealing apps.

It seems pretty sneaky for Foursquare to require you to enter an ID you literally can't access if you want to opt out.

However, when Apple hid the IDFA, it also introduced a new privacy feature called App Tracking Transparency that requires apps to obtain explicit user permission before accessing the identifier.

Making sure your IDFA is set to private on your Apple devices should keep them out without you having to dig for your ID. If you are on an OS earlier than iOS 14, go to Settings, navigate to Privacy, select Advertising, and set your IDFA to private. For iOS 14, Apple requires apps to ask for a user's permission to track them the first time they open the program. Disable and deny all these

requests by going to *Settings, Privacy & Security*, then *Tracking*, and turn off "Allow apps to request and track."

BASH THE BROKERS BY…LEAVING THE LISTS

People-finder sites and giant data brokers aren't the only way your private information is sold and used. Here's how to get your name removed from postal lists, telemarketing lists, and more.

How to remove your name from postal mail lists

Direct mail firms bristle at the term "junk mail." If it's personalized and contains a useful offer, they reason, it's not junk. But I counter with this: If it gets immediately thrown into the recycling bin, that's *the definition of junk*. So here's how to stop junk mail in its tracks.

Go to the top

The easiest way to get off direct mail lists is to opt out at DMAChoice, the consumer preferences service run by the Direct Marketing Association. It costs $7 to remove up to three household members' info for 10 years. (When I wrote the first version of this guide in 2023, it was $5 for five household members.)

Return to sender

Some organizations—such as companies you've done business with in the past and charities—aren't required to remove you from their lists. But you don't have to accept every piece of mail that finds its way into your mailbox.

According to the USPS, unless a piece of mail was sent registered, certified, or the like, you can simply write “Refused” on it and put it back in the box for the mail deliverer to pick up.

If the sender is smart, they’ll remove you from their mailing list. This process will probably be slow, but over time it should make an impact.

My mail deliverer told me they are not allowed to accept “Refused” or “Return to Sender” mail that’s addressed to “Current Resident” or “Your Name or Current Resident.”

Another easy (but also slow) tactic is to write “Remove me from your mailing list” on the offer, stick it into the pre-paid reply envelope you’ll find in some direct mail packages, and send it right back to them.

Be proactive

Still getting junk? You could also use PaperKarma’s mailer directory to search for instructions on how to stop the worst direct-mail offenders. The directory is not comprehensive, but it does include major mailers like AARP and MasterCard.

How to remove your name from prescreened credit offer lists

The companies that generate your credit score—Experian, TransUnion, Innovis, and Equifax—do more than influence whether (and how much) credit you get. They also sell your data to businesses that target you with financial offers.

OptOutPrescreen.com is "the official Consumer Credit Reporting Industry website to accept and process requests from consumers to Opt-In or Opt-Out of firm offers of credit or insurance."

Opt out either for five years (by opting out online) or permanently (by opting out via post), and you'll no longer be included in "firm offer lists" provided by these four consumer credit reporting companies.

How to remove your name from Valpak coupon lists

If you're tired of getting those packs of (mostly useless) coupons in your mailbox, unsubscribe here.

How to remove your name from all postal mail lists

If you prefer to have someone else handle all your postal mail opt-outs, try PaperKarma—an app that not only unsubscribes you from general direct mail lists, but also removes your name from the lists of charities, local mailers, catalogs, credit and insurance companies, and more.

The service costs $24.99 per year. If you go this route, ignore the advice above for removing yourself from various postal lists...this app will do it for you.

How to remove your name from email lists

The DMA also runs the fast and free Email Preferences service: just enter up to three email addresses, and they'll be made available to all advertisers that use the service to clean their lists.

This won't stop spam, as actual spammers notoriously don't care if you want to receive their crap. But it's a start.

How to remove your name from telemarketing lists

The U.S. Federal Trade Commission runs a national Do Not Call Registry. It's free and will get you off the sales lists of "real companies." In other words, it won't protect you from scammers, who aren't interested in your calling preferences.

BASH THE BROKERS BY…SPREADING DISINFORMATION

No, I don't mean posting misleading political memes on Facebook. I mean throwing red herrings into data scrapers' databases…in other words, poisoning your data. I got this idea from Michael Bazzell's book *Extreme Privacy*, and have been doing it off and on when I'm bored and have time to spare.

Two things to try:

1. *Fill out forms or order items with your real address and phone number but an alias name*. When the company invariably sells your info, it now looks like someone else lives at your address. (Even better if you manage to remove your real name from the lists; but even if you don't, you now have a roommate who doesn't exist.)

2. *Fill out forms or order items with your real name but a fake address, email, and phone number*. Bazzell offers a lot of detail on how to create your alias information without accidentally using a real person's info.

   This tactic is especially useful if you have an unusual name, since you're easier to find; creating "more" of yourself can throw marketers and others off your trail.

Enhance the effect by posting the alias contact details on your social media profiles and websites, uploading a CV to resume sites, etc.

This works great with all those “freebie” and “make money from surveys” sites that ask for your race, religion, product preferences, and more. I filled out an eight-page survey saying I listen to techno, enjoy MMA, go fishing regularly, and have four cats.

Chances are, within a few months you’ll find your alias information propagating onto the people-finder lists.

To find out what the internet knows about you, both before and after a disinformation campaign, ask ChatGPT. You’ll need to create an account to get the best results, so use a masked email address—and delete your data and your account when you’re finished with it.

Ask ChatGPT where you live, what you look like, etc., and request the sources of any information it brings up; this may help you uncover more places to remove your data, take down photos, etc.

CHAPTER 7

SURF IN SECRET

Disengaging from the internet completely is a pipe dream for most of us. If you can't (or don't want to) stop surfing the internet altogether, take steps to ensure that as little of your data as possible is being leaked to data brokers, scammers, and marketers...and that you're providing the minimum amount of free labor to Big Tech.

SURF IN SECRET BY...REWRITING YOUR LIFE STORY

You've created a professional bio for your job or business, or maybe you've filled out the profile sections on hobby sites, special-interest websites, online communities, and so on. And now the innocent act of sharing information about your life is coming back to bite you in the butt—because it's been scraped, harvested, and leaked. Here's how to rein your bio back in.

Step 1: Edit (or delete) your bios

Plug your name into a search engine to see what profiles and bios pop up. Then log in to the sites as needed to delete your information. (Or seed them with disinformation, as we discussed above.)

It's not always easy. For example, editing my "Knowledge Page" on Google was literally impossible. My

correspondence with customer service went nowhere, and Google switched my bio to one I used years ago and started displaying an incorrect birth year. I'd be happier if I could control the bio more directly, but will have to be OK with them sharing outdated, incorrect information.

Step 2: Control your data on sites you don't control

What if information about you appears on websites you have no control over? Sometimes, all you have to do is ask nicely that your details be removed or updated.

As a former business owner, I spilled details about my life in bios and interviews everywhere from print magazines to podcasts. I contacted blogs I guested for as long as two decades ago to ask them to change my online bio to a more generic, less personal version, which I sent along with my request. Most of them did.

I also asked website owners to remove interviews from my past life as a business owner—but only if the interviews were outdated or contained more personal information than I'm now comfortable with sharing. I understood I was asking people to take time out of their day to delve into their website and remove information I previously agreed to have there, so I tried to keep the requests to a minimum (and was very polite about it).

For example, I didn't bother going after a case study an old client included me in. The case study is fairly up to date, it shares valuable information, and it isn't overly

personal. While I would rather have the case study gone, it's not important enough for me to bother the website owner about.

(As a side note, I've been pleasantly surprised at how many people complied with my requests.)

Step 3: Ask Google to stop serving up your old info

So you've gotten your bios removed or edited. But Google still shows the old info when you do a search!

Google Search periodically reindexes sites to ensure the search engine has the freshest information. Speed this up by using this link to ask Google to remove or reindex outdated content. (You do need to have a Google account for this.) Check back later to see if your request has been approved or denied.

I used this method to ask Google to reindex the contact page on my site when I switched to a masked email address, and also to remove old results from a business I no longer own.

Want to go the extra mile? Here's how to get search engine results deleted from Bing and Yahoo.

(DuckDuckGo uses Bing and Yahoo, among other services, to help provide search results—so information deleted from these search engines will likely disappear from DuckDuckGo as well.)

SURF IN SECRET IDEA BY...CONTROLLING YOUR (ACTUAL) IMAGE

If you're a typical internet user, your photo is everywhere. Your employer's "About Our Staff" page. Facebook. Google's image search. And so much more. The bad news: These photos are being used to train AI in facial recognition, which may later be used to surveil us.

According to NBC News:

> Facial recognition can log you into your iPhone, track criminals through crowds and identify loyal customers in stores.
>
> The technology—which is imperfect but improving rapidly—is based on algorithms that learn how to recognize human faces and the hundreds of ways in which each one is unique.
>
> To do this well, the algorithms must be fed hundreds of thousands of images of a diverse array of faces. Increasingly, those photos are coming from the internet, where they're swept up by the millions without the knowledge of the people who posted them, categorized by age, gender, skin tone and dozens of other metrics, and shared with researchers at universities and companies.

If this technology doesn't scare you, consider this: Anyone can surreptitiously snap a photo of you, upload it to any number of free services, and find your social media profiles and other information about you. Anyone can find out you were involved in a protest, even if you were wearing a hat or glasses. Someone could use your Instagram selfie to figure out where you live.

Sure, these systems are also used by law enforcement to protect innocent people…but being on the right side of the law doesn't mean you're immune from being targeted by an online posse you somehow pissed off.

You may not want to (or be able to) change or delete some of your online photos. Your employer might not be cool with you having a blank square as your professional headshot, and you're not allowed to remove photos from your friends' Instagram accounts. For safety reasons, a group that meets up in person may require that your profile have a real photo before they'll let you join. You'll also need a professional headshot on LinkedIn if you're looking for a job.

But in many cases, it's either simple to change your photo or the company or website doesn't need to have it at all. (A doctor's office recently asked me to add a photo of myself to their portal. Why?)

Here are some ideas for controlling your image.

Get creative

Have some fun with it! I changed one photo of me to a photo taken during a costume party. (Even PimEyes—see the box below for more on them—didn't bring up any results from this photo.) On other sites, I swapped out my photo for random photos or artwork.

Ask nicely

If your photo is on a website you don't control, ask the site owner if they'd be willing to take it down. Sometimes it's a simple oversight, like an old employer who forgot to remove you from their "About Our Employees" page.

Get the law on your side

Google will remove photos of you that are inappropriate or harassing. There's a special process to follow for this situation, and the images must meet three criteria:

1. The imagery shows you (or the individual you're representing) nude, in a sexual act, or in an intimate state.
2. You (or the individual you're representing) didn't consent to the imagery or the act and it was made publicly available OR the imagery was made available online without your consent.
3. You are not currently being paid for this content online or elsewhere.

Here's where to request the removal of images meeting these criteria.

If the images don't meet those criteria, you may still be able to get them removed by making a request under the Digital Millennium Copyright Act to remove unlawful material.

Opt out of spy services

Two platforms that have many of us concerned are Clearview AI and PimEyes, facial recognition search engines that are scarily accurate.

I uploaded to PimEyes a recent photo of myself that exists only on my phone, and the search engine pulled up photos of me going back at least 10 years, including a photo of myself with my young child at an art studio. Anyone who finds the photo can narrow down where I live since the studio website includes their address.

Luckily, you can opt out. You'll be required to upload an image of your face plus an anonymized scan of an ID.

- PimEyes Opt Out
- Clearview AI Opt Out

Before requesting removal, it may be worth it to pay for a month's worth of PimEyes' advanced service to get the actual URLs of the photos it turns up in order to request removal from those sites if possible.

Ask friends to not share or tag your images on social media

You can be extra careful about your online image…and have it all wrecked when a well-meaning relative tags you in a group photo on Facebook.

I have at least two friends who make a point of asking during gatherings that no one post photos of them online, and as far as I can tell, they've never experienced any pushback. You might ask that, at a minimum, friends and family don't tag you in the photos they post.

Just say no to the TSA

When an organization or corporation asks for your biometric information, just say no.

At the airport TSA booths at the security check-in, there are signs stating that you may opt out of their scans.

From my searches on the topic, I can see that many people are afraid to exercise this right. But most people who do opt out never experience any pushback to a polite "I'd like to opt myself [and my family, if applicable] out of the biometric scan."

I did have one TSA agent tell me the images are not stored, but that's only a half truth: Some images are stored for training purposes. Not only that, there's no stopping them from eventually deciding to store (or share) this information.

Or they may leak it. In 2019, 184,000 traveler images were stolen in a data breach when "U.S. Customs and Border Protection did not adequately safeguard sensitive data on an unencrypted device used during its facial recognition technology pilot," according to the Council of the Inspectors General on Integrity and Efficiency.

To make things worse, a 2019 study showed that Asian and African American people were up to 100 times more likely to be misidentified than white men by facial recognition technology.

If you're privileged enough to be unafraid to exercise your right to opt out of TSA scans, this tiny act of resistance can help those who are not. While it's doubtful that the small percentage of travelers who opt out are going to sway TSA policy, it's easy to do—and the person behind you in line may be emboldened to do likewise.

Strip metadata from your images

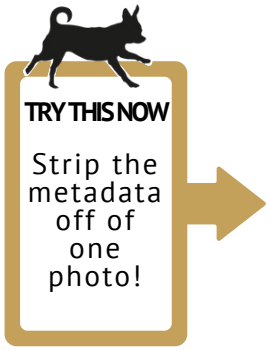
If you do post photos online, you might want to strip out the metadata first. Metadata is information embedded within the file that indicates what kind of camera you

used, what editing features you used, the time and date you took the photo, and even the coordinates of the location where you took the photo.

Why is this a problem? According to PrivacySavvy:

> [People] could use it to stalk and harass you online and offline, while others could mount social engineering and phishing campaigns to steal your identity. While some companies, such as Instagram, have tried to erase metadata from publicly available photos, the data is still stored in their servers, and they can use it for their own benefit. Also, hackers can breach their servers and access your data, compromising your privacy.

Remove metadata manually on MacOS using one of these methods:



- Open the file in Preview, save it as a PDF, then open and save the PDF as a jpeg. Crop as needed.
- Take a screenshot of the photo, crop as needed.
- Download the free app Photo Anonymizator. To process the photo, right-click on the filename and select *Open With…Photo Anonymizator*.
- Download the free, open source app ImageOptim. Open the app, drag and drop in the photo file, and click *Anonymize*. You can even use the settings to have the app automatically anonymize the file name and choose a new creation date.

I have tried all of these methods. Photo Anonymizator is the easiest, but ImageOptim offers more features. Changing the file type and taking a screenshots are a minor pain in the butt, but they don't require an app.

Remove metadata manually on Windows using these instructions:

1. Click the *Details* tab.
2. Click the *Remove Properties and Personal Information* link.
3. Select *Create a copy with possible properties erased*.
4. Click the *OK* button.

Android and Apple phones don't offer a way to do this. Thankfully, however, there are apps that can quickly delete or change photo metadata on your computer *or* phone, often in bulk:

- For Android: EXIF Editor (Free)
- For iOS: EXIF Metadata (Free
- For Windows: Exif purge (Free)
- For MacOS: Photos EXIF Editor ($3.99)

Corporations like Meta (owner of Instagram and Facebook) have enough of our data already. Stripping the metadata from your images keeps them from deriving even more information from your online activity.

SURF IN SECRET BY...USING A VPN

VPN stands for Virtual Private Network. In short, it's an encrypted "tunnel" between you and the VPN's servers. All your internet activity is routed through the tunnel, and even your own ISP can't see it. When you use a VPN, no one can see your IP address—the string of numbers that identifies your device. Instead, they see the IP address of the server your traffic is being routed through.

VPNs are great not only for minimizing how much you're tracked and the amount of data being collected about you—they also let you use free wi-fi hotspots more safely.

VPNs don't guarantee anonymity, but they do close off one big point of access to your info. Advertisers, for example, can still track you with trackers and cookies, even by recognizing the unique setup of your browser. (More on this later.)

I use the VPN bundled with my ProtonMail subscription (for more info on Proton, see Chapter 21: Say Goodbye To Google). This VPN was rated Best Open Source VPN for 2025 by CNET. Others in the top include:

- ExpressVPN (Best VPN Service Overall)
- NordVPN (Best for Speed)
- Surfshark (Best Cheap VPN)
- Mullvad (Best Privacy VPN)

Prices vary depending on the service and how many months you're willing to commit to it. In addition, many VPN companies run deals, such as for Black Friday. I've seen prices ranging from $1.99/month to $12.99/month.

Wondering if your VPN is really concealing your location? Visit DNSleaktest.com and the site will instantly display the IP address and city you appear to be coming from. If it's your actual IP address and city, you know your VPN isn't working.

Free VPNs exist, but at best they will restrict data, speed, and features—and at worst they may make their money by selling your data, hitting you with ads, or even installing malware on your computer. Not that they're the only danger: Even some of the paid VPNs are fakes meant to steal our money, bandwidth, or data. To make sure you're avoiding scam VPNs, check out this VPN Warning List from the digital privacy advocacy group RestorePrivacy.

SURF IN SECRET BY...THROWING OUT THE COOKIES

Cookies are bits of data websites store on your computer so that the next time you visit, the website will remember you.

First-party cookies are meant to make your browsing

experience better—for example, the website will remember your preferences—and the data remains on the website you're using. Third-party cookies, however, transmit your data to outside businesses so they can track and advertise to you. (That's why some ads seem to "follow" you around the web.)

Here's how to keep cookies from tracking you and sharing your data. Before you follow any of these instructions, first consider whether you'd prefer to replace your current browser with a privacy-oriented one; it would be a waste of time to redo all your settings on, say, Chrome, only to switch to a cookie-killing browser later.

Option 1: Refuse cookies

An easy way to put the kibosh on third-party cookies is to simply not allow them. Some websites will display a pop-up or slide-in asking if it's OK for them to use cookies. Choose "necessary cookies only" to allow the website to use only the cookies that enhance your browsing experience, while disallowing third-party cookies.

Option 2: Opt out of cookies on a case-by-case basis

If a website doesn't display a pop-up allowing you to decline cookies, check the website's cookie policy, which is sometimes rolled into its privacy policy. This document may offer information on whether (and how) you can opt out of cookies.

Some websites have a handy "Do Not Sell or Share My

Personal Information" link at the bottom of the page to let you quickly opt out of cookies.

Option 3: Disable all cookies

It's also possible to disable cookies in your browser altogether. This has the disadvantage of also rejecting the cookies that make websites work. You'll need to re-log into every service you use each time you use it, and may need to occasionally turn cookies on to use all of a website's features.

Here's how to reject cookies in the most popular browsers. You usually need to quit and restart your browser for the changes to take effect. These instructions are for the browser you use on your computer, not your other devices; the steps for deactivating cookies from your preferred browser app may be different.

How to disable cookies in Firefox

1. In the Menu bar at the top of the screen, click *Firefox* and then select *Preferences or Settings*.
2. Select *Privacy & Security*.
3. In the *Enhanced Tracking Protection* section, select *Custom and then Cookies*.
4. Use the drop-down menu to choose the type of cookies to block.
5. Close the *Settings* page. Any changes you've made will automatically be saved.

How to disable cookies in Chrome

1. At the top right in your Chrome browser, select *More*, then *Settings*.
2. Select *Privacy and security*, then *Third-party cookies*.
3. Select *Block third-party cookies*.

How to disable cookies in Safari

1. Go to *Settings*
2. Go to *Advanced*.
3. Check the box *Block all cookies*.

How to disable cookies in Microsoft Edge

1. Select *Settings and more* in the upper right corner of your browser window.
2. Select *Settings* then *Cookies and site permissions*.
3. Select *Manage and delete cookies and site data* and disable *Allow sites to save and read cookie data (recommended) to block all cookies*.

When you disable cookies in your browser, future attempts to place cookies on your computer will be blocked.

Option 4: Let browser extensions do the work

An extension—sometimes also called an add-on or a plug-in—is software that adds features to your browser.

Extensions are typically easy to install, and once you've done it, they'll work for you seamlessly in the background.

Use a free tracker-blocking browser extension and you'll be amazed at how many cookies and other trackers it intercepts every day. I use Privacy Badger, which was created by the nonprofit digital rights organization Electronic Frontier Foundation. It's easy to install and works great. To find a free cookie-crumbling extension for your browser, check out Chapter 18: Annihilate Ads.

EMPTY THE COOKIE JAR

You chose one of the methods above to keep websites from putting cookies on your computer. However, cookies can hang around for a long time, so it's a good idea to clear out the ones that are already there.

These instructions are for the browsers on your desktop computer and not your mobile devices. Keep in mind that when you clear cookies, you may be logged out of any websites you're signed in to.

How to clear cookies in Chrome

1. At the top right in your Chrome browser, click *More*.
2. Select *Delete browsing data*.
3. Choose a time range, like *Last hour* or *All time*.
4. Select the types of information you want to remove.
5. Click *Delete data*.

How to clear cookies in Safari

1. In Safari, choose *Safari*.
2. Select *Settings*.
3. Select *Privacy*.
4. Click *Manage Website Data*.
5. Select websites, then click *Remove* or *Remove All*.

How to clear cookies in Microsoft Edge

1. Go to *Settings*.
2. Select *Privacy*.
3. Select *Clear browsing data*.
4. You can also select *Ctrl+Shift+Del* or type *edge://settings/clearbrowserdata* in your address bar to access this function.

How to clear cookies in Firefox

1. Click the menu icon, click *History*, then click *Clear Recent History*.
2. Set *When:* to *Everything*.
3. Select *Cookies and site data*.
4. Click *Clear*.

The steps for deleting cookies may be different in each browser's phone app. In all cases, you may need to quit and restart the browser for the changes to take effect.

Even more troubling than third-party cookies are supercookies. There are two types, and they're both difficult to get rid of.

One type of supercookie is a Flash cookie. Check out this guide on removing Flash supercookies from your computer.

The other type is placed on your computer by your Internet Service Provider. The ISP sells the data to third parties—and even worse, they can restore deleted cookies. The only way to block them is to run a VPN on your computer.

SURF IN SECRET BY...FIGURING OUT YOUR FINGERPRINT

Can someone pinpoint you by the unique fonts on your browser, the content filters you use, your screen resolution, your add-ons, or the local time on your device?

With enough data points like these, yes, they can.

The Electronic Frontier Foundation offers a browser fingerprint test called Cover Your Tracks. Just click *Test Your Browser* and Cover Your Tracks "shows you how

trackers see your browser. It provides you with an overview of your browser's most unique and identifying characteristics."

It's enlightening (and frightening) to see how all your browser data can converge to make you uniquely identifiable.

If you discover you have a unique fingerprint—which you likely will—and this bothers you enough to take action, CyberInsider offers suggestions for mitigating it. I followed the instructions for Firefox and the process was quick.

Add-ons can spoof your browser to show snoopers different metrics than your actual set-up. For example, if you're on Safari with a Mac, the add-on might show you're on Chrome with a tablet. But not only do these add-ons break some sites, the spoofed profile might make you even more identifiable.

If you want to try one anyway, CyberInsider recommends finding one that lets you change profiles, like Chameleon for Firefox, and cycling through different profiles at random intervals.

CHAPTER 8

ESCAPE EMAIL TRACKING

Email: We're either addicted to it, or wish it would go away. Or both!

We're drawn to it due to the promise of intermittent rewards: Most of the time we get nothing good, but every once in a while we hit the jackpot, such as a job offer, a note from a friend, a deep discount, or a funny photo. That promise keeps us hopeful…and always checking.

The heaviest 25% of email users spend almost nine hours per week on email, according to Microsoft. That's 19 full days pre year you're subtracting from your life. Worse, everyone from small-time spammers to our corporate overlords use email to track, target, and harass us.

In Chapter 21: Say Goodbye To Google, we'll talk about ditching your email provider for a more privacy-forward one. In the meantime, here are some ideas for getting less email—thus decreasing the amount of time you have to spend on it—and protecting your data and privacy.

ESCAPE EMAIL TRACKING BY…INSTALLING PIXEL BLOCKERS

Whenever you open an email sent by a business or marketer, chances are you're being tracked. How? They

embed a one-pixel image at the end of their emails that sends back data on when you opened the email, how many times, and even from what city. They may also track whether you clicked on any links.

This is mostly used for legitimate purposes; for example, a business may want to know which of its emails got the most opens or which links got the most clicks in order to provide better content and offers. Not to mention, some people just like to track whether their emails are being seen.

It sounds fairly harmless, and you may not care if Kohls knows you clicked on a coupon, but a critique from Mike Industries points out some concerning pixel-tracking scenarios:

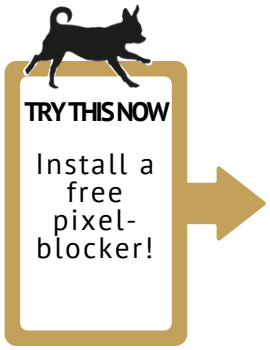
- A stalker ex knowing you opened an email in the morning in California and in the evening in New York, broadcasting the fact that you're not at home.
- A creep sending your child a Minecraft guide they refer to often, in order to track them throughout the year.
- An email marketing provider deciding to license data to third parties, including location data and timestamps—and that third party using the data to target you, or even sublicensing the data to other third parties.

If you don't want information on your whereabouts and

online activity shared, you could change your email settings to block external (or remote) images; just open up the settings and dig around for this option. But if you go this route, you would need to click to see any image in an email, such as a photo from a friend.

A more elegant solution is to install a pixel blocker on your browser. This does exactly what it sounds like, and even lets you know when an email attempts to track your actions.

Here are a couple I've used and liked:



- PixelBlock is a free Chrome and Firefox extension. The best part is the little red eye icon it displays on an email to let you know the extension blocked at least one tracking attempt.
- Ugly Email is another free Chrome extension with an eye icon, and it works in much the same way as PixelBlock.

If you use another browser, search for "[Browser Name] pixel blocker" to see what extensions are available. Most extensions will walk you through set-up.

ESCAPE EMAIL TRACKING BY...CREATING A BURNER EMAIL

Whether you use a free email like Gmail or Yahoo or have an address in your own personal domain, it's typically

easy and free to create additional email addresses to give to businesses and people you have no reason to trust.

ESCAPE EMAIL TRACKING BY…MASKING YOUR EMAIL ADDRESS

A masked (or anonymous) email address hides your information while forwarding emails to your email address. When you send mail through these addresses, the service provider encrypts the email and also hides personally identifiable information like your device name and IP address. Even better, it's easy to delete a masked address if you start getting spam there—which isn't so easy with your real email address.

I've used two services to create masked email addresses:

- DeleteMe, the company I used to remove my family's info from people-search sites. Masked emails (and phone numbers and credit cards) come with the service, so why not?
- ProtonMail, my secure email provider, which also offers masked emails with its paid subscription. Their browser extension will even let you create masked addresses on the fly when you're confronted with a form asking for your email.

Any service you try will provide information on how to create masked emails.

You can even create a new masked address for every purpose. Both Proton and DeleteMe let you turn off addresses as needed, and there doesn't seem to be a limit on how many you're allowed to make.

Using a different email for each login can make a mess of your passwords. Unless you have a password manager like LastPass, 1Password, or Proton Pass, you'll need some way to store or remember which address you used on what accounts when you sign in.

If you're likely to change your mind about the whole thing, don't go overboard creating anonymous addresses. You'll just have to change them back. Instead, create just a few masked email addresses for various uses.

The idea of using masked emails is not just to protect your personal information, but also to confound Big Tech. I love the idea of a broker having an entry for me with 50 email addresses. If I'm really lucky, maybe all this is causing data brokers to maintain multiple entries with different names and emails, few of which are actually attached to me.

I have no idea if it works that way...but one can hope.

ESCAPE EMAIL TRACKING BY…USING A PRIVACY-FORWARD EMAIL PROVIDER

Instead of, or in addition to, using masked emails, you might want to switch to a secure email provider. Here are some inexpensive and free services:

- Proton offers—on the free plan—an email address, up to 10 "hide-my-email" aliases, three calendars, up to 1 GB storage, and more. I was able to quickly import my old emails, contacts, and calendars from Gmail. I pay $14.99/month for more features and two members, but have noticed they occasionally run sales.

- Tuta is a "free and secure email service that lets you create an email account with built-in encryption for maximum data protection." I was told by someone in the know that Tuta is actually more protected than Proton. The free email includes a calendar and 1 GB of storage. Upgrading (€3/month—that's $3.12 as of February 2025) gets you additional features, such as auto-reply, alias emails, and the ability to use your own domain.
- Mailfence offers "No ads, no spams, no trackers, no solicitations, no backdoor," and state-of-the-art security features. The free version gives you 500 MB of storage for emails and 500 MB for documents. The top tier plan ($3.50/month) will get you more storage, the ability to use a custom domain, and more.

- Posteo provides “a secure, ad-free email account powered by 100% green energy” for just €1 ($1.04 as of February 2025) per month.

Many of the secure email providers are based in EU countries, which have stronger privacy protections. These are only a few of the most common ad-free, anti-tracker providers; a quick search for “secure email provider” will bring up many more.

ESCAPE EMAIL TRACKING BY...USING THE “+” TRICK

Create different, custom email addresses in Gmail, Outlook, or MS Exchange by adding a “+” symbol to your address and appending other characters. For example, if your Gmail address is xyzabc@gmail.com you might provide your email for a Nike discount as xyzabc+nike@gmail.com. Emails to this address will still reach you.

If you start getting unwanted mail at this subaddress, set up a filter to automatically delete any emails sent there.

Marketers know this “one simple trick.” It’s trivially easy for them to clean their mailing list to remove the portion after the “+” symbol. So use this tactic only as a last resort if the other ideas here don’t work for you.

CHAPTER 9

PROTECT YOUR PHONE

Smartphones may be the world's best tracking devices: They collect our data, share our details, and know everywhere we go. And yet, they've become a necessity. Below, you'll learn how to protect your data, safeguard your privacy, and thwart scam calls.

PROTECT YOUR PHONE BY...GETTING A MASKED NUMBER

Mask your phone number using a service like DeleteMe or MySudo (which charges $.99 per month for one anonymous phone number plus other perks). This lets you generate anonymous numbers that will ring on your real line.

PROTECT YOUR PHONE BY...USING SPAM BLOCKER APPS

Spam blocker apps, such as Robo Shield, Truecaller, and Robokiller, not only block many telemarketers and scammers—some of them, usually in the paid versions, also play an "out of service" recording to encourage the caller to remove you from their list.

Be sure to check the privacy policy before installing; I once uninstalled a spam blocker when I discovered it was sharing my data for marketing purposes.

PROTECT YOUR PHONE BY...TRYING TEMPORARY TEXT NUMBERS

You try to create an account for an online service and they ask for your mobile number to verify your sign-up. If you're already pretty savvy about protecting your data, you may try a burner Google Voice number or free SMS number site—but you quickly discover that the company asking for your number is more savvy than you, and they reject the anonymous digits.

One solution is veritel.io, an "online service that provides access to physical SIM cards via a virtual interface." According to the site, "Our primary aim is to offer an alternative to physical SIM cards, enabling users to receive text messages online for various purposes such as verification, activation, and confirmation on various platforms."

You're priced by the number, and the price varies depending on the country the number is in and the service you're looking to sign up for. For example, to get a U.S.-based number to confirm your LinkedIn account, you will pay 76 cents. An Austrian number for use on Google will cost $2.70.

I haven't tried this service, but my understanding is that these numbers work well to fake out online services/verification systems/etc.—and if the number you purchase doesn't work, the company refunds your credit so you can try another one.

PROTECT YOUR PHONE BY...HIDING YOUR LOCATION

Investigative reports have shown that your phone's location data may be for sale. And it's not just where you shop people are interested in; according to the Electronic Frontier Foundation, "Multiple data brokers have specifically targeted and sold location information tied to reproductive healthcare clinics."

If you'd rather not have details on your whereabouts gathered and sold for commercial or punitive purposes, it's important to control your phone's location tracking.

Here's how to turn off tracking on your mobile phone (and, for good measure, on your laptop).

It's difficult to know if a stray app is tracking your location—or if your phone manufacturer is simply lying about whether your tracking is on. Not to mention, your phone can be tracked even when it's off or in airplane mode.

If you're serious about not being tracked via your mobile phone or laptop, look into purchasing a Faraday pouch. This is a bag that prevents signals from being sent from or received by your device.

Keep in mind if you disable location services completely, you won't be able to use maps and other apps that rely on location data. If this is a problem, instead turn off location access for individual apps. (After all, why does a game or podcast app need your location?)

How to disable location tracking on iOS

1. Go to *Settings*.
2. Select *Privacy*.
3. Select *Location Services*.
4. Turn off location sharing.

How to disable significant locations on iOS

1. Open *Settings*.
2. Select *Privacy & Security*.
3. Select *Location Services*.
4. Select *System Services*.
5. Select *Significant Locations*.
6. Tap *Clear History* to delete your recorded locations from all your Apple devices using the same Apple ID.
7. Turn off Significant Locations.

How to disable tracking for specific apps on iOS

1. Go to *Settings*.
2. Select *Privacy*.
3. Select *Location Services*.
4. Choose the apps and services you want to stop sharing with.
5. Tap the app name, then under *Allow Location Access*, select *Never*.

How to disable location tracking on Android

1. Swipe down from the top of the screen.
2. If the location icon is highlighted, tap it to turn it off.
3. There will be a warning that some apps may not function properly. Confirm by tapping *Close*.

How to disable tracking for specific apps on Android

1. Swipe down from the top of the screen.
2. Touch and hold the location icon.
3. Tap *App location permissions*.
4. Find the apps that can use your device's location.
5. To change an app's permissions, tap it and then choose the location access for that app.

How to disable location tracking on MacOS

1. Click the Apple menu.
2. Go to *System Settings*.
3. Click *Privacy & Security* in the sidebar.
4. Click *Location Services*.
5. Turn off Location Services.

How to disable location tracking in Windows 11

1. Go to *Start*.
2. Select *Settings*.
3. Select *Privacy & security*.
4. Select *Location*.
5. Switch the *Let apps access your location* setting to *Off*.

While you're in these settings on your various devices, also look for the option to delete location history. Then do that too!

If you're afraid to turn off location tracking altogether, keep in mind this is easy to reverse if it starts affecting features and apps you need.

Some apps will keep asking you to restore location permission. If this happens to you, the only solution (besides turning location tracking back on for the app) is to toss the app and get a different one.

PROTECT YOUR PHONE BY...BEING CHOOSY ABOUT APPS

The apps on your phone—especially free ones—collect reams of personal data. According to Surfshark:

> Social media apps share secrets, while the food delivery category is a data glutton. Both categories tracked an average of 20 out of 32 possible data types. Shopping (18 types of data), Dating (16 types), and Payments (15 types) round out the top five categories.

And those are the ones that are operating above-board and haven't been compromised by bad guys. In early 2025, reports Wired, "a hack of location data company Gravy Analytics has revealed which apps are—knowingly

or not—being used to collect your information behind the scenes."

More from the article:

> Some of the world's most popular apps are likely being co-opted by rogue members of the advertising industry to harvest sensitive location data on a massive scale, with that data ending up with a location data company whose subsidiary has previously sold global location data to US law enforcement.

Some of the apps involved included games like Candy Crush and Subway Surfers, transit apps, period-trackers, MyFitnessPal, Tumblr, Yahoo email, Microsoft's 365 office app, and even religious apps and VPNs. (A good reason to avoid free VPNs!)

It's scary to think about the types of data we input into apps, which can then collect it, combine it with data from other sources, and share it with third parties far and wide.

Personal finance apps get a sneak peek into our income, debt, and spending patterns. Health trackers know everything from how much we exercise to whether we missed our meds today. Period tracker apps can tell if we're pregnant or perimenopausal. Diet apps know what we eat and when. Shopping apps can glean all sorts of details about us based on what we buy, where, and when.

The only ways to safely use many apps are to give them false information…or to not use them at all. If there's an app you can't do without, check out their privacy policy and be sure to opt out of data sharing wherever possible.

Some apps are worse than others when it comes to data-grabbing. Take a look at Mozilla's Privacy Not Included guide for privacy ratings of various apps, websites, and products.

The only ways to safely use many apps are to give them false information…or to not use them at all. If there's an app you can't do without, check out their privacy policy and be sure to opt out of data sharing wherever possible.

PROTECT YOUR PHONE BY…BLOCKING (ALMOST) EVERYONE

When I had an iPhone, I blocked calls from anyone not in my contacts list. When someone not in my contacts list called, the phone would not ring and the call would go straight to voicemail. (And scam callers almost never left a voicemail.)

It was rare that I missed a legitimate caller—and when I did, I just checked the voicemail and called them back. The

ability to protect my peace and quiet was worth the few instances of legit missed calls.

Other types of phones have this feature, but I wasn't able to find a clear answer on whether the callers could leave a voicemail or were *block*-blocked. If you have another brand of phone, it might be worth testing out.

CHAPTER 10

STOP BEING LOYAL

You're about to buy a mattress online, and a pop-up appears offering you a discount in exchange for your name and email address. You enter the info, and a second pop-up asks you to enter your text number to claim the discount.

Or maybe you're at the bookstore, and they offer a free tote bag if you sign up for their loyalty program.

I used to work with both the marketing and retail industries, so take it from me: The point of a loyalty program isn't (only) to reward your loyalty as a customer. It's also to harvest your data. Many of these companies run a brisk second business selling your information, which marketers slice and dice to learn more about you.

You may be thinking, "There's no way my friendly local supermarket is harvesting and selling my data." But as just one example, according to The Markup, "Kroger has carefully grown two 'alternative profit business' units that monetize customer information, expected by Kroger to yield more than $1 billion in 'profits opportunity.'"

One billion dollars...from collecting and selling *your* data!

If you're fortunate enough that you can afford to not trade your data for bonuses, discounts, sale notifications, and other perks, consider whether it's worth joining loyalty schemes. Do you really use Kohl's cash? Do you need the bonus points from Dick's Sporting Goods? Is it worth buying into your own exploitation to get a few bucks off your Brookline sheets?

If trading your data for dollars seems like a sweet deal, the good news is that once you've put some of the privacy practices from this guide into place, these tactics will help you protect some of your data while still getting the perks. Use a masked email address, enter your secondary phone number, give them your PO box, change your name. (I discovered my grocery store will let me use any name…the address of the store itself as my "home address"…and a random 10-digit number.)

These data points may still wind up attached to your personal profile—for example when you use your credit card at the supermarket, revealing your true identity—but at a bit of disinformation might at least help obscure the real stuff.

PART 3

DISENGAGE BY...RECLAIMING YOUR HOME

Big Tech doesn't see you only when you're online. They can find you at home and look right into your house, too. Here, you'll learn how to hide your home photos, keep your address private, and stop smart home products from sharing your private data.

CHAPTER 11

HIDE YOUR HOME ADDRESS

You may already have gotten your data deleted from people-search sites...but your home address lives in other places online as well. Here are a couple of ways to keep your address mum.

HIDE YOUR HOME ADDRESS BY...GOING PO

When you're getting food delivered, requesting a taxi, or ordering from an online store, of course these businesses will need to know your home address. But there are many instances where a business doesn't need this information. For example, your bank, car insurance company, and grocery store don't need to know where you actually lay your head at night.

One solution is to get a PO box, and to use it anywhere you don't need to input your actual home address.

When I was looking into this, I discovered virtual PO boxes. These are real addresses, but you don't have a physical box. The virtual PO box service collects your mail and sends you photos via email or in their app. The company will trash mail pieces for free, or charge a small fee to hold your mail for pick-up, email a scanned PDF of the contents, or shred it. The company I tried, iPostal1, offers discounted bundles of scans/shreds.

My advice is to not go this route until you've:

- Gone through the businesses and websites on your spreadsheet and requested they stop sending you marketing mail. (Chapter 5: Control Your Online Accounts has more info.)
- Removed yourself from data broker lists where possible. (See Chapter 6: Bash The Brokers.)
- Signed up for the Direct Marketing Association's Do Not Mail list. (See Chapter 6.)
- Signed up for paperless billing, statements, etc. where possible.

This way, you're not getting a ton of mail to your virtual PO box that you may have to pay to have scanned or shredded.

Once you have a PO box, whether virtual or physical, switch over to this address for all businesses that don't need to know your home address.

To be transparent, I didn't love the experience. I frequently received ads at my PO address such as credit card offers, which I then had to pay to have shredded. (Remember, Do Not Mail lists do not apply to companies you currently do business with.) It was also more of a pain than it was worth for me to have a delivery address that was different from my billing address, as I now needed to enter two addresses any time I used my credit card online.

In the end I cancelled by PO box and went back to using my home address, but this idea may work better for you.

HIDE YOUR HOME ADDRESS BY...ADDING DISINFORMATION TO THE SYSTEM

If you, like me, decide not to use a PO box, try this instead: Create an alias mailing address and use it with your real name, and create an alias name to use with your real address. We discussed this In Chapter 6: Bash the Brokers.

HIDE YOUR HOME ADDRESS BY...CHECKING OUT PUBLIC RECORDS

Your home address may be visible online in the form of public records and, unfortunately, you often can't delete your address from these sources. For instance, many states keep open records on home sales. As another example, if you registered a business using your home address, your state may not allow you to change or delete the business records they make available to the public online.

Worse, people-search sites get a lot of their info from public records, making it even more difficult for you to wrest control of your home address from these companies.

If you have a court order because you've been stalked or are otherwise in danger, send it with your request for deletion from public records. Then follow up, follow up, follow up.

If you *don't* have a court order and simply want the records changed for future safety and privacy considerations, you may be out of luck. The only thing you can do is try: Reach out to the website, government office, or whatever it is and politely ask how to have your personal data removed.

Many voter sites do offer a way to opt out of having your home address visible. However, the site may still announce, "See how Maya's neighbors on Gardenia Grove Drive voted!" Real helpful.

There is a bright side: Now that you know all this, you'll take pains to conceal your home address in future dealings. In his book *Extreme Privacy*, Michael Bazzell even recommends buying a home in the name of a trust instead of using your own name. This may not be useful information now, but it's something to consider if you're ever in the market for a new home.

HIDE YOUR HOME ADDRESS BY...BEING MASTER OF YOUR DOMAIN

If you own a domain name (such as www.example.com), anyone can do a WhoIs search to find out who owns the domain plus their address, phone number, and email address.

Every domain host I've used has offered privacy protection, either free or paid. When you turn this setting on, the WhoIs lookup for your domain will show the contact information for your domain host instead of your personal details.

You do need to provide your domain host with a working email address (even if it's a masked email) to abide by the law and so the host can contact you about your payments.

CHAPTER 12

REMOVE YOUR HOME PHOTOS FROM THE WEB

Did you know it's incredibly easy for people to see images of the inside of your home online? Sites like Realtor.com, Redfin, and Zillow display interior photos from the listing when you bought your house. This means strangers can see the layout of your home's interior.

While real estate sites let randos see inside your home, Google Street View and Apple Maps Street View let them view the outside. These photos may include personal possessions like your car, bike, toys in the yard, and identifying flags such as a Pride flag, state flag, or college football banner. (They do blur out license plates.)

Here's how to keep people from peeking into your home.

STEP 1: CLAIM YOUR HOME TO DELETE INTERIOR IMAGES

Real estate listing sites will let you "claim" your home, at which point you can remove the listing photos.

Anyone who knows just a few simple details about you can pass the verification to claim your home…so if you haven't done it, do it now.

Here's how to claim your home on the most popular real estate websites. You will need to create an account, or log in if you already have an account.

How to claim your house on Zillow

1. Go to the How Much is My House Worth? page.
2. Type in your address.
3. Click *Claim this home* in the pop-up box.
4. Follow the instructions to complete claiming the home.

Zillow requires you to confirm via email before they'll allow you to remove your images.

How to claim your house on Redfin

1. Go to the Claim Your Home page.
2. Enter your address.
3. Follow the instructions to complete claiming the home.

How to claim your house on Realtor.com

1. Go to the My Home page.
2. Enter your address.
3. Follow the instructions to claim the home.

The fact that it's so easy to claim ownership of a house is another good reason to get your home address removed from the web wherever possible.

STEP 2: BLUR YOUR HOME IMAGES IN STREET VIEW APPS

If you don't like the idea of online strangers being able to glean details about your personal life from exterior photos of your home, ask Google Street View and Apple Maps Street View to blur your home's image. This is irreversible, so make sure you really want to do it...for yourself and for anyone who lives there in the future!

There is some debate about whether you should blur your home on maps apps. Some say it makes you stand out more, and some point out there are other ways to see your home online anyway...so why bother?

Despite all this, you may want to blur your home as a middle finger to surveillance capitalists.

How to ask Google to blur the image of your home

1. Open Google Maps.
2. Find and open the 360 photo that shows your home.
3. In the bottom right, click *Report a problem*.
4. Complete the form.
5. Click *Submit*.

If you enter your email address, Google may contact you for additional information.

How to ask Apple to blur the image of your home

Email mapsimagecollection@apple.com with your request. Be sure to include the full address of the home, the coordinates (which you can find by searching for your address in Apple Maps), and any other information that will help them locate the image.

CHAPTER 13

BANISH SMART PRODUCTS FROM YOUR SPACES

We're being sold the "dream" of totally hands-off homes. What this means for you is you're able to check in on your dog, turn on your lights, or lock the doors no matter where you are.

What this means for the businesses that provide these products is that they have access to very personal details about you and your life. This information isn't protected by default, so businesses can be privy to your comings and goings (from your smart doorbell), the layout of your home (from your robotic vacuum), and even when you're sick (from your oral thermometer).

Imagine what they can infer about you from the combination of data they snatch from your home. It would be easy to know you're on vacation just from the patterns of your door lock, lights, and alarm. Digital creepers can see when you're depressed from the books you're reading on your Kindle, the movies you're watching, your decline in treadmill use, and the fact that you haven't left your house in a week.

Some smart products are even actively sharing your data with outsiders. The Atlantic reports:

> Some security-camera companies share information with police departments. [D]epending on your settings, your smart speaker may use your voice data—including coughs, snores, baby gurgles, and barks—to sell you more products. Not only that, some gadgets may be able to siphon data from your personal wi-fi network and send it back to the company.

Worse, many of these products provide little security; while researching this chapter, I came across a Redditor whose home assistant accidentally paired with his neighbor's Bluetooth toothbrush.

"I now know when my neighbor is brushing his teeth, which gives me a good idea when he gets up and when he goes to sleep," the poster wrote. "Probably [I could deduce] when he is not at home (e.g. vacations) and I can also see how much pressure he is applying and which program he is using."

In the intro to this guide I talked about how difficult it is to remember a time when you could go about your day without the feeling of being constantly surveilled. Knowing that these intrusive technologies are tracking you even in your home, you can understand why, if it's feasible for you, smashing the smart home is such important work.

FIRST, SURVEIL THE SURVEILLORS

Take a look around your home and make a list of all the smart products—items that are potentially storing, sharing, and exploiting your data. Consider your:

- TV
- Car
- Light switches/lightbulbs
- Refrigerator
- Alarm
- Locks
- Heating/AC systems
- Remotes
- Printer
- Oven
- Microwave
- Doorbell
- Security camera
- Speakers
- Coffee maker
- Thermostat
- Toothbrush
- Vacuum
- Tablet
- E-reader
- Fitness tracker
- Digital camera
- Digital personal assistant
- Exercise bike, treadmill, etc.
- Smoke/CO detector
- Dishwasher
- Oral thermometer
- Gaming console
- Washer
- Wi-fi-enabled headphones
- Dryer

These are only some of the more common smart products you may have in your home; this list is just meant to get you started.

Once you have your list, for each applicable product:

Step 1: Ask yourself whether the product really improves your life

In other words: Do you really need or want to have this in your home? Maybe you have a disability or mobility needs, so it's useful to be able to turn on and off lights, set your alarm, and lock the doors through an app. Or the smart treadmill helps you stay motivated to exercise by tracking your progress, and you don't want to give that up.

You may discover, though, you have a lot of products that don't add enough to your life to give up your data for them. For example, I didn't get much benefit from a smart thermometer connecting to an app on my phone, so why continue to use it? It was easy enough to replace it with an old-school one.

Step 2: Update the privacy settings for each product you keep

Change the privacy settings in any apps associated with your smart products to the highest protection level. You may also need to check the settings on your smartphone to ensure the products aren't accessing features they don't need—like your camera, microphone, location data, or contacts list.

Step 3: Delete conversations

Ever talk to Siri or Alexa, or any other device or app? Get rid of your conversation history.

According to PCMag, there have been reports of Amazon employees actively listening to Alexa voice recordings. Google speakers have also been compromised, exposing users' private conversations.

The easiest solution for many people is to just not use personal digital assistants. But these products are lifesavers for some of us.

If you're pretty skilled with tech, consider a privacy-forward, open-source assistant like Home Assistant, which is "perfect to run on Raspberry Pi or a local server," though you can also run it on MacOS, Windows, and Linux. The company website offers thorough documentation and getting-started guides, but the learning curve looks steep.

Here's how to delete your conversation history on Alexa, Google Assistant, and Siri. It makes sense to do this periodically to decrease the chances of your home chatter being compromised by the companies providing these apps (or by criminals).

How to delete your Alexa voice history

1. In the Alexa app, open *More*.
2. Tap *Settings*.
3. Select *Alexa Privacy*.
4. Select *Review Voice History*.
5. Set the date to *All history* and tap *Delete all of my recordings*.

How to delete your Google Assistant history

1. Go to your Assistant activity page.
2. Sign in to your Google Account.
3. Tap *More*.
4. Select *Delete activity by*.
5. Select *All time*.
6. Tap *Delete*.
7. To confirm, tap *Delete*.

It may take a day before the activity is deleted from your other devices.

How to delete your Siri history on iOS

1. Open *Settings*.
2. Go to *Siri* (or *Apple Intelligence and Siri*).
3. Tap *Siri & Dictation History*.
4. Tap the *Delete Siri & Dictation History* button.
5. Confirm by tapping *Delete Siri & Dictation History*.

How to delete your Siri history on MacOS

1. Open *Settings*.
2. Go to *Siri* (or *Apple Intelligence and Siri*).
3. Click the *Delete Siri & Dictation History* button.
4. Confirm by clicking *Delete*.

For instructions for other Apple devices, read this article.

Step 4: Tell them to stop eavesdropping

Starting with iOS 13.2, you have the power to choose whether you want contractors to listen to your Siri interactions in order to improve the service.

To opt out of Siri recordings review on MacOS

1. Open *System Settings*.
2. Go to *Privacy & Security*.
3. Go to *Analytics & Improvements*.
4. Turn off *Improve Siri & Dictation*.

To opt out of Siri recordings review on iOS

1. Open *Settings*.
2. Tap *Privacy & Security*.
3. Tap *Analytics & Improvements* at the bottom of the screen.
4. Turn off *Improve Siri & Dictation*.

You may need to delete recordings separately from Apple CarPlay, your smartwatch, etc. These steps will keep Apple employees from listening in on your conversations with Siri.

Step 5: Keep your printer private

Home printers are one of the most egregious invaders of our privacy. They aren't necessarily "smart," but many of them send your data back to the manufacturer (aka "phoning home").

Cory Doctorow writes about the printer HP charges you a monthly fee to use (after you buy it!): "When you click through the signup agreement, you grant HP permission to surveil every document you print—and your home wifi network more generally—and to sell that data to anyone and everyone."

And according to Epson's privacy policy, the company collects "data about the type of device or browser you use, your device's operating software, printing patterns, ink usage, warranty status, your internet service provider, your device's regional and language settings, and device identifiers such as model number, age, and IP address."

Some of this is for benign purposes, like being able to warn you if your ink is low. But Epson makes clear in their privacy policy that the data they collect from you may also be processed for advertising and marketing purposes.

Ready to get these corporations out of your private spaces? Two ways to keep your printer from phoning home are:

- *Find a printer that lets you decline tracking* as you're setting up the software. It's hard to know if that will be the case until you start actually installing it, but you may be able to ask others about their experience before buying a printer.
- *Use a USB-only printer* (which connects directly to your computer) instead of a wireless one—meaning it's not attached to your internet network at all.

Neither of these are ideal. What would be truly ideal is for corporations to let you control the product you paid for, and for them to not use products you own as data harvesting devices. But they're a start.

Install a free, open source printer driver, such as Gutenprint for MacOS or OpenPrinting for Linux; there don't seem to be many for Windows except perhaps CUPS, which looks fairly complicated for a single user with a single printer. You'll need to find a driver that works with your printer; the three here support many different brands and models.

Step 6: Put your smart products on a guest wi-fi network

A guest network is a secondary network isolated from the home wi-fi your laptop and mobile devices are on.

Putting your smart home products on a guest network helps keep businesses and people from accessing your home network through these products.

If you have a newer router, you may already have an app for managing your wi-fi network; in the settings, simply add a new network, choose a name for it, and create a password.

No app? Log into your wi-fi using any device, then open the network settings to find your router's IP address. For Android, it's under the wi-fi settings. For Mac, click on the wi-fi symbol and then select Open Network Preferences.

Enter your router's IP address into your browser; once you get to the page, enter your credentials to log in. From there, you may have to click around to find the right page or tab to create a guest network.

If you can't find your router's IP address or have other difficulties, check the sticker on the bottom of your router for information that can help.

Once you have a guest network ready, the next step is to get your smart home products set up on the new network; refer to the user manuals for instructions. It was fairly easy to get my robotic vacuum and printer moved over to the new network, so I hope the process is fast for you as well.

Step 7: Tell your car to stay in its lane

Printers are bad, but cars are worse. Anyone who tracks your car knows when you're out of your house, what establishments you frequent, and where you are whenever you're on the road.

To find out what data your car is collecting and sharing, enter your vehicle's VIN at the Vehicle Privacy Report website. Tighten up your privacy choices or ask the manufacturer to delete your data based on the information you find.

When I discovered that my car may track and share location data, I tried calling the number listed in the manufacturer's privacy statement and was on hold for ages...and then disconnected. I ended up sending a letter via post, and received a response via mail over two months later.

Step 8: Rinse and repeat for all your smart products

There are too many smart products and too many ways to adjust them to fit into this guide. Check each device's privacy policy to know which invasive features to turn off, and set each device to the strictest privacy settings in their respective apps.

PART 4

DISENGAGE BY...RECLAIMING YOUR CONTENT

We often say "we are the product" of companies like Facebook, LinkedIn, Twitter/X, Google, and other sites—but that's not quite correct. The product is *the stock*, and *we* are the unpaid workforce.

As Douglas Rushkoff writes in *Survival of the Richest: Escape Fantasies of the Tech Billionaires*:

> We dutifully read, click, post, and retweet; we become enraged, scandalized, and indignant; and we go on to complain, attack, or cancel. That's work. The beneficiaries are the shareholders.

A platform becomes more powerful the more people join it. Your free content draws new people into the fray, the platform locks them in ("all my friends and content are there!"), and it becomes that much stronger...all so its shareholders can rake in more dollars at your expense. In this section, you'll withdraw your content from Big Tech, and learn how to make it work for *you* instead.

CHAPTER 14

PROTECT YOUR POSTS

One type of content you're donating to for-profit businesses is forum posts. Not only do your posts help attract more users and more engagement for the platform, but the business gets to harvest your data as well.

Do you really want data brokers, and the marketing firms they sell to, knowing that you belong to a personal finance forum, a community for people with diabetes, or a *Twilight* fan fiction writers group? Going further, would you want them to know what you post on these sites? Just imagine your health insurance provider being privy to your posts on the diabetes forum.

I'm not saying anyone should feel ashamed about the forums they belong to or what they post there. What I'm saying is that anything you share online can be scraped by businesses to enrich your profile…and possibly to be used against you.

Here's how to minimize the amount of unpaid labor—and data—you provide to these businesses.

OPTION 1: ERASE USELESS POSTS

I discovered that in many cases, there was no point at all in my posts remaining online. For example, say I asked a question in 2015, it was answered, and the post has had zero views in the last five years, meaning no one is getting any value from it. Why not delete it?

When you delete a Reddit post, it can still be accessed by anyone with the direct link. People can use platforms like Reveddit to uncover all your "deleted" content.

Even if you delete your entire Reddit account, your posts stay live but with the username deleted.

I have successfully used the Redact tool, which, instead of deleting posts, comments, DMs, and chats, replaces them with a random series of words. They offer a free plan plus paid plans that let you delete more posts and from more sites.

OPTION 2: DELETE FORUM ACCOUNTS ALTOGETHER

If you want to disengage even more, delete some of your forum accounts altogether. This is another

instance where it makes sense to balance your need for community with your need for privacy.

Maybe you're okay with the world seeing the information you've shared on one forum, but not the juicy details you've spilled on another. Or you're fine with sites that let you sign up with minimal personal information. Or a particular discussion group is simply so important to you, the benefits outweigh the disadvantages.

Note that, as with Reddit, deleting forum accounts may or may not also erase your posts. Check out the forum's policies, and if they specify that posts are not removed when you delete your account, go through first and delete your posts one by one. If you want to be super careful, obfuscate your posts before closing your account.

This method isn't foolproof—there are ways people can find deleted posts if they want to, such as by using the Wayback Machine.

Again, we can never achieve 100% privacy and anonymity—even if it's what we want to do. My philosophy is to do as much as I can, and to be more careful in the future based on what I learned going through the process.

OPTION 3: POST YOUR CONTENT ON YOUR OWN WEBSITE

If you really like to share, why not post your wisdom, advice, thoughts, and ideas on a platform you control? More on this in Chapter 16: Say Sayonara to Social Media.

CHAPTER 15

RETRACT YOUR REVIEWS

Another type of content we create for free—and that megacorps profit from—is reviews.

I'll never forget this scene from an episode of South Park:

Barkley: Sir, it's midnight. Go home, get some sleep.

Sgt. Yates: There's no time to sleep when the city's counting on me.

Barkley: More Yelp reviews, sir?

Sgt. Yates: I had a bad experience at Red Lobster and if the people don't know about it, they could too. Folks deserve to know where to eat, Mitch.

Barkley: But does anyone even thank you for it?

Sgt. Yates: I don't need them to. I know they need me, and that's enough.

Barkley: God bless you, sir.

Sgt. Yates: I know.

We feel like we're doing a good deed when we post a review warning people away from a restaurant whose servers *just don't care*, or pointing them to a stellar gym. But what did we do before there were so many outlets for us to share our yeas and nays? Somehow we all survived.

When you spend time writing a review of the local skate park, you're working for the review site. Your Google reviews give Google data. Information from Yelp is used to train data analysts. Amazon reviews keep people on, well, Amazon—and unscrupulous sellers game the system with fake reviews anyway, so why bother?

Also, recall that one side benefit to disengaging is being able to see the world through our own eyes, without automatically framing all of our experiences for online consumption. Habitual reviewing trains us to see every experience as just more fodder for strangers' eyes (and data scrapers' databases).

When I decided to disengage as much as I could, I deleted all my reviews. (Thank goodness there were only four.)

Now, whenever someone asks me for a review, I ignore it; if they persist, I tell them I don't write reviews as a policy.

If this resonates with you, I urge you to delete all your reviews from these sites:

- Facebook and other social media
- Yelp
- Tripadvisor and other travel sites
- Amazon
- Goodreads (owned by Amazon)
- Home services review sites like Angi and Thumbtack
- The Better Business Bureau
- General review sites like Trustpilot
- Software review sites such as Capterra
- Employer review sites like Glassdoor

In most cases, you can remove a review by logging into the service and navigating to your profile or settings. Here are a few exceptions:

- Remove Google reviews from the Google Maps site.
- Yelp will ask you for the reason you're requesting removal. Selecting "I changed my opinion of this business after a new interaction" might be the best route. (It's the only one that doesn't make you *or* the business look like a jerk.)

- The Better Business Bureau does not seem to provide an easy way to remove complaints or reviews. Your best bet is to find your local BBB office at BBB.org and call them to find out.

Really, really want to write up a glowing review or slam a business that did you wrong? In Chapter 16: Say Sayonara To Social Media, you'll learn about a method for posting content to your own site and syndicating it on social media.

I inadvertently did this when, instead of complaining on a review site when a business ripped me off to the tune of $10,000, I wrote a 5,000-word report about my experience, posted it on my business website, and then shared the link on social media.

A minor celebrity retweeted the link, and my story racked up over 20,000 hits in one day. It also garnered media coverage and spawned *65 pages* of comments.

Can you imagine a review on Trustpilot getting that much response? Sharing my content on my website ended up being a much better way to warn people than a handful of snippy reviews on other sites.

CHAPTER 16

SAY SAYONARA TO SOCIAL MEDIA

What a minefield: We know how bad social media is for our mental health. We know that these platforms mine, use, and sell our data ruthlessly. We know their algorithms serve us negative, frightening, or rage-bait stories—and sometimes just plain lies—because that's what gets engagement.

Since I wrote the first version of this book, things have gotten much worse. Let's take a look at just a few examples.

What's wrong with Twitter?

Twitter, now X, has become the mouthpiece of an angry billionaire who is currently taking over the U.S. government—slashing departments and aid while raking in money on government contracts.

What's wrong with TikTok?

In late 2024, TikTok's main feed showed "a high volume of…not attractive subjects"—so the company changed its algorithm to boost users it considered better-looking. The company also quantified the amount of time it takes for someone to get addicted—260 minutes, or about 35 videos—and it wasn't so they could stop it.

What's wrong with Meta/Facebook/Instagram?

This is just a tiny bit of the news that came out in early 2025 about this company:

- Meta's Facebook and Instagram are getting rid of their moderation teams.
- Meta torrented terabytes worth of pirated books to train its AI.
- In early 2025, Meta suffered a backlash when it introduced AI profiles to Facebook and Instagram; these fake profiles were sloppy, lied to users, and were occasionally racist.

So why do we have such a hard time quitting social media?

For some of us, Facebook is the only way we can stay in touch with far-flung friends and families. We need LinkedIn for our jobs. We feel there are no good alternatives for selling our art (Instagram!), moving our books (TikTok!), or generally promoting our businesses (YouTube!).

Reddit gives us a community to belong to when there are none near us IRL. And without Nextdoor, how can we passive-aggressively shame our loud neighbors, find out why there's a white van in our driveway, or ask whether that snake is a copperhead?

There is another powerful reason we have trouble letting go of social media, and it was articulated perfectly by Nicholas Carr, the author of Superbloom, in The Art of Manliness podcast in January 2025. (Lightly edited.)

> In the physical world if you're quiet in a social setting...you're still there, you're still present. Online, if you go quiet, you disappear. That's another reason we're encouraged to constantly post things, express ourselves, put up pictures. There are studies that show that if you compare people conversing online versus people conversing in person, people online tend to divulge four times as much information about themselves in a given period of time.

That's a tough one to solve. After all, who wants to feel as if they've disappeared? Tackling this issue could fill a whole book on its own, but hopefully the advice below will help you shake the feeling that if you're not online, you're not anywhere.

See the ideas below to determine whether it's possible for you to disengage from social media, where to go instead, how to run a business without it, and how to use social media while giving up as little data as possible.

GET REAL ON THE PROS AND CONS OF SOCIAL MEDIA

If you're interested in spending less time online, protecting your personal data, and giving the bird to Big

Tech, take a good, hard look at whether social media is serving you. Some platforms may be indispensable to you, while others are a waste of your precious attention and life energy. Here are some questions to ask yourself:

Question 1: How much does social media help me with my career?

Think about the millions of people screaming to be heard on social media. Your posts are swept into oblivion within seconds by the sheer number of new posts. Are you really getting enough return on your investment of time and energy?

(If you do decide you need to be on social media for your career or business, check out "Option 2: You Want to Stay on Social Media" later in this chapter for tips.)

Question 2: Are there other ways to accomplish the tasks I use social media for?

Whether you're using a social platform to communicate with friends, market your business, or just to be entertained, think about what other platforms and places are available for meeting these needs.

For example, instead of selling items on Facebook Marketplace, can you save it all up until you have enough for a yard sale? If you have a side gig as a dog walker, would it make sense to ditch Instagram and instead post signs and ask local veterinarians to mention you to clients?

If you're doubtful that your career can survive without social media, run a time-limited experiment to see whether any offline marketing techniques will work for you; you may even find one you enjoy, which means you'll do more of it. If we managed to do these activities before social media existed, there must be some ways to do them now without relying on those platforms.

Question 3: What am I missing by seeing everything through a camera lens?

As Nicholas Carr said above, sometimes we feel social media is as crucial as oxygen because we've been trained to think that everything we do and think has to be visible to others, lest we not fully exist. It's not hard to guess who trained this into us, and how they benefit.

Until a couple of years ago, I had an Instagram account to post my photography. I wasn't selling it…I just wanted validation from other people. When I realized how absurd this was and deleted my account, I was also freed from the small, insistent voice in my head saying, "Ooh, I should post this!," "I wish I had gotten that on film," "I need to check for likes and comments!" and "I should probably interact with other people's posts so it doesn't look like I'm only here to post my own photos…which I am."

Are you missing out on your life because you're constantly thinking about how to frame everything you do, think, or see for social media?

It's a nice feeling to experience something exceptional and not automatically think, "I should put this on Facebook." Experiencing something in real life and not through the lens of a camera gives you a sense of quiet confidence, knowing you can do and experience amazing things and not need to prove it to the world.

Question 4: Does anyone *really* care if I'm on social media?

As I mentioned, I opened an Instagram account just to post my photography. I was more interested in gaining other people's approval of my photos than in giving approval myself. I'm not unique; chances are, many other people are using social media in the same way.

When I quit Facebook, Twitter, and LinkedIn in 2015, I had *thousands* of friends and followers. In the weeks following my departure, which I didn't announce, only two people noticed I was gone.

I know we all want to imagine that people will weep in their beds if we leave social media. But the harsh fact is, for most of us it's not true.

Question 5: Do I need the information I get from social media?

I have never seen anything on Nextdoor that has changed what I think or do. The same goes for Facebook memes, TikTok videos, and Instagram photos. In fact, after I take them in, I wish I could get those seconds of my life back.

Ask yourself when was the last time you actually heard or saw something useful or actionable on social media—and, more importantly, whether you used or took action on it.

Question 6: Are my connections close enough friends for me to deal with the hassle?

If I have to find out from Facebook that you got married, graduated college, won the lottery, or had a baby…we're probably not very close friends. Close friends call, or at least text, with big news.

Sure, there are people who are more than acquaintances but not quite good friends, but I don't need to invest hours of my time—and my mental health—scrolling through my feed to make sure I don't miss their latest news. (I wouldn't expect them to do it for me, either.)

If you feel guilty quitting these platforms because you need them to stay connected with friends, consider whether they are close enough friends for you to want to deal with the data mining, invasions of privacy, misinformation, and blows to the self-esteem that are an integral part of social media.

Again, when I quit social media in 2015, it was crickets. No one sent messages asking, "Where have you been? We miss your pet photos, humblebrags, homemade memes, and random musings on life!"

Maybe you're more popular than I am, but I suspect most people on social media are doing exactly what we're doing—worrying about themselves.

Question 7: How do social media companies benefit by making me feel like I've disappeared if I'm not on their sites?

This goes back to the quote from Nicholas Carr. Why is it important to social media platforms that you're on there as much as possible, as opposed to popping in once a week to check your feeds? What do they get out of it, and is their gain your loss?

Let's say your answers to the above questions have convinced you to leave social media. Here's how to do it. (Later in this chapter, we'll talk about what to do if you decide to remain on social platforms.)

OPTION 1: YOU DECIDE TO CLOSE YOUR SOCIAL MEDIA ACCOUNTS

Take a deep breath! I'll walk you through the whole process. Remember, you can always quit one at a time—or some and not others—if that feels better for you.

Step 1 to Quitting Social Media: Let your friends know

No one likes those "I'm leaving Facebook forever, goodbye!" posts...especially when the person sheepishly reappears three weeks later.

Instead of dramatically announcing your departure, inform the people you actually want to stay in touch with that you're leaving the platform and suggest alternate ways to continue communication—such as via text, phone, email, or a better social platform (which we'll discuss later).

If you belong to a group that uses a specific social platform to make plans, share news, and so on, suggest moving the whole group somewhere else.

Signal is a good replacement for iMessage, Facebook Message, Skype, and other chat groups. The app includes messaging, group chats, voice and video calls (including group calls), and even messages that disappear once the recipient reads them. Everything Signal offers is end-to-end encrypted—and it's free and open source.

Step 2 to Quitting Social Media: Download your data

Before you click "Close My Account," be sure to download any photos, posts, and other information you want to keep.

Keep in mind that the data you will receive may vary; for example, LinkedIn let me download my recommendations and some other data, but I ended up copying and pasting all my posts into a document by hand.

You'll need to be logged in on your desktop browser to start a download request. Some sites let you download your data right away, while others will email you a download link. Unless otherwise indicated, It can take up to 30 days to receive the email; if you close your account before then, you won't receive your data.

How to download your data from Twitter/X

1. Select *More* in the main navigation menu.
2. Select *Settings and privacy*.
3. Choose *Your account*.
4. Select *Download an archive of your data*.
5. Confirm your password, then select *Request archive*.

It looks like posts are not included with the data you download; if you want them, you'll have to copy-paste or find another method. I attempted to download my data from a test account and never received the emailed verification code.

How to download your data from Facebook

1. Click the down arrow under your profile picture.
2. Go to *Settings & Privacy*.
3. Select *Settings*.
4. Scroll down to *Your information* and click *Download your information*.
5. Click *Continue* to visit the Accounts Center.
6. Click *Download or transfer information* in the pop-up.
7. Choose which information to download. Click *Next*.
8. Choose how much information to download and click *Next*.
9. You'll be asked whether you want to download the data to a device or transfer it elsewhere. Make the selection and click *Next*.
10. Click *Submit request*.

How to download your data from Instagram

1. Click on your profile picture.
2. Select *Settings*.
3. Scroll down to the *Security* section.
4. Click on *Download Data*.
5. Choose the type of data you want to download.
6. Select the export format; HZD will give you a ZIP file with your data.
7. Confirm the download.

How to download your data from TikTok

1. Click the three dots next to your profile picture.
2. Click *Settings* and scroll down to the *Account* section.
3. Choose the type of data you want to download.
4. Select the export format.
5. Click the *Download* button.

How to download your data from Pinterest

1. Click the down arrow on the top right corner of your screen.
2. Select *Settings*.
3. Select *Privacy and data*.
4. Under *Request your data*, click *Start request*.

It may take up to 48 hours to receive a download link. Do not close your account before your data download request is complete.

How to download your data from Reddit

1. Visit https://www.reddit.com/settings/data-request.
2. Log in to the Reddit account you'd like to request data from.
3. Select the reason for your request and a date range or *All Time*.
4. Click *Submit*.

How to download your data from Threads

1. Click the two-line menu in the bottom left.
2. Select *Settings*.
3. Click *Account*.
4. Click *Download your information*.
5. Enter the email address where you'd like to receive a link to your data, then click *Request Download*.
6. Enter your Instagram account password and click *Next* in the top right, then click *Done*.
7. You'll receive an email titled *Your Threads Data* with a link to your data. Click *Download data* and follow the instructions to finish downloading your information.

How to download your data from Discord

1. Go to *User Settings*.
2. Select *Privacy and Safety*.
3. Click the *Request all of my Data* button.

It may take up to 30 days to receive a download link. Do not close your account before your data download request is complete. If you're wondering, this is the data you will receive.

If you're on a social site not listed here, look up "How to download data from [site]."

Step 3 to Quitting Social Media: Delete your content

If you want to be extra careful, once you have your backup in hand, delete all your content before closing your accounts. We know that deleted posts from Reddit are still searchable...and who knows what other sites will do with your content once you close your account?

If you were a prolific social media user, deleting all your posts manually can take for-ever. Here are some ways to make it happen.

For Twitter/X, try TweetDeleter. This service starts at $2.99 per month.

The free version of Redact works for Reddit, and, to a limited extent, for a couple other platforms. The premium version (at $14.99/month) lets you delete more content, and also works with Discord, Twitter, Facebook, Imgur, Tumblr, Bluesky, and many more—even some dating and productivity sites. Check here for the full list.

Another idea is to delete a handful of posts each day when you need a break from other work. It may take longer that way, but is not as much as a burden.

Step 4 to Quitting Social Media: Close your accounts

Here's how to close accounts on the most popular social media sites.

In some cases, your account will not be closed right away; for example, Facebook takes 90 days to delete all your data, Pinterest takes 14 days, and Twitter/X takes 30 days. If you log in again during the process, your account will be restored.

Afraid to let go? Facebook, Instagram, Pinterest, and LinkedIn, and probably others, let you temporarily deactivate your account.

When you start to follow the steps in the links below to delete an account, the platforms will usually first ask if you'd like to deactivate it temporarily instead, and then walk you through the process.

For the instructions below, you'll need to be logged into the site on your desktop browser.

How to close your Twitter/X account

1. Click on the *More* icon.
2. Select *Settings and privacy*.
3. From the *Your account* tab, click *Deactivate your account*.
4. Click *Deactivate*.
5. Enter your password.
6. Click the *Deactivate account* button.

How to close your Facebook account

1. Go to your Accounts Center and click on *Personal Details*.
2. Select *Account ownership and control*.
3. Select *Deactivation or deletion*.
4. If you have both Facebook and Instagram accounts, you'll be asked to choose one.
5. Here's where you have the option to temporarily deactivate your account. Otherwise, select *Delete account* and click *Continue*.
6. Keep hitting *Continue* through all the pleas for you to stay until you get to the actual deactivation option.
7. Enter your password.
8. Hit *Delete account*.

If you don't log in again for 30 days, Facebook will permanently delete your account. If you want to check that your account has been deleted, ask a friend on the platform to see if they can find your profile. I once discovered my account was still not deleted a year after I went through the process!

How to close your Instagram account

Do the same as for Facebook above, but select Instagram instead of Facebook. Deleting the Instagram account associated with Threads will also delete your Threads account if you have one.

How to close your Threads account

1. Click the two-line menu in the bottom left.
2. Click *Settings*.
3. Click *Account* at the top.
4. Select *Deactivate or delete profile*.
5. Click *Delete profile*.
6. Follow the prompts, then click *Delete Threads profile*.

How to close your Pinterest account

1. Click the down arrow at the top-right corner.
2. Select *Settings*.
3. Select *Account management* from the left-side navigation.
4. Click *Delete account*.
5. Click *Continue*.
6. Select the reason you're leaving, then click *Send email* to receive an email to delete your account.
7. Check your email to confirm.

How to close your Discord account

1. Go to *User Settings*.
2. Select *My Account*.
3. Select *Account Removal*.
4. Click *Delete Account*.
5. If you're a server owner, you'll need to either delete the server or transfer ownership.
6. Enter your password and your six digit 2FA code.
7. Click *Delete Account*.

How to close your Reddit account

1. Go to *Account Settings*.
2. Scroll down to the *Advanced* section and click *Delete Account*.
3. Enter the required details and check the box that says *I understand that deleted accounts aren't recoverable*.
4. Click *Delete*.
5. If your account was created with your Google account or Apple ID, scroll down to the *Account authorization* section of your account settings and click *Disconnect* next to the Google account or Apple ID you signed up with. If you don't have a password yet, you'll be asked to create one.

How to close your LinkedIn account

1. Click the *Me* icon at the top of your LinkedIn homepage.
2. Select *Settings & Privacy*.
3. Go to the *Account preferences* section.
4. Under the *Account management* section, click *Change* next to *Close account*.
5. Check the reason for closing your account and click *Next*.
6. Enter your account password and click *Close account*.

If you don't log in again within 14 days, your account will be permanently deleted.

If you belong to any platforms not listed here, search for "how to delete [site] account" to find instructions.

Once your account is closed, you may find that Google will still show your posts in search results. This will stop happening over time as Google updates its data, but if you don't want to wait, revisit Chapter 7: Surf in Secret for details on how to remove outdated results in Google, Bing, and Yahoo.

OPTION 2: YOU WANT TO STAY ON SOCIAL MEDIA

For those who can't say goodbye forever to social media, the ideas below will help you reap the benefits, while minimizing the amount of data, content, and attention these companies can extract from you. I'll list these from the simplest to the most complicated.

Set a limit

Like to relax on social media, but worry about getting trapped in the infinite scroll? Ask someone you trust to change the password to your account and only give it to you if you really need it (as defined in advance by you). This works for any type of website you want to use only occasionally, but have trouble dragging your attention away from.

If that's too hardcore for you, try a site-blocking app like AppBlock (Android/iOS), Freedom (Android/iOS), or SelfControl (MacOS). These let you add distracting sites

to a blocklist, and many apps let you set time limits for different sites as well.

Ditch the apps

The social apps go everywhere you go...and some of them track you the whole time. If you simply have to use social media while on the go, log in via the website using the browser on your phone.

Choose your platform wisely

If social media is necessary for your job or business, consider which sites are best for your purposes. Usually, those are the ones you like enough to really work at.

For instance, I realized the majority of my clients came through LinkedIn. So rather than spreading myself thin trying to reach audiences through all social sites at once, I doubled down on LinkedIn. It worked so well that even after I deleted my LinkedIn account, I continued getting reach-outs from prospects who had seen me there!

Move to the fediverse

A big problem with the dominant social media platforms is that they "trap" you there. If you leave, you lose your content and your connections.

But for almost every one of these platforms, there's an analogous social media site that won't trap you—in what's called the *fediverse*.

What the fediverse? According to The Verge, it's "an interconnected social platform ecosystem [...] which allows you to port your content, data, and follower graph between networks."

In other words, imagine if you could post on TikTok from your Facebook account. And if you decided to leave Twitter/X, you could transfer all your connections and posts to Instagram.

Here are some platforms to check out. They all have good features...and a surprising amount of traffic.

- Instead of Twitter/X...try Mastodon or BlueSky. (This platform is not yet fully interoperable because it uses a different type of fediverse protocol. But as of now it *is* interoperable with Mastodon.)
- Instead of Reddit...try Lemmy.
- Instead of Instagram...try Pixelfed.
- Instead of YouTube...try PeerTube.
- Instead of Facebook...try Friendica, Hubzilla, or Diaspora.
- Instead of Goodreads (owned by Amazon)...try BookWyrm or The StoryGraph.
- Instead of Discord...try Mattermost or Signal. (You can install and start using Signal in seconds, while Mattermost is more of a DIY set-up better for tech-savvy people.)
- Instead of TikTok...sign up for a beta of Loops.

If you move to one or more of these federated social platforms and get your friends and family to move there as well, the site will grow. Over time it will be so much like the old social media—minus most of the bad parts—that you won't miss the old ones at all.

Not sure which site to try? The Fediverse Observer can help you narrow down the best sites and servers for your needs.

Threads is sometimes mistaken as a friendlier version of X/Twitter, but it's owned by Meta—the same company that owns Facebook and Instagram. You need to have an Instagram account to sign up for it. With all these federated social media sites listed above, I see no reason to join Threads.

Fake them out

Some social platforms let you choose an anonymous username. Even if they don't, you're likely to get away with using at least a semi-fake name. When I took a course that used a Facebook Group, I created an account using my first and middle names, and didn't post a photo or any personal information.

While you're at it, change up the info in your account: Use a masked email, PO box, burner phone number, etc.

Refuse to share

Want to (or have to) have a public profile? Be careful about what and how much you share. Even if you're required to be on the platform, say for work, you aren't required to get personal. When you do post or comment, keep the personal details light.

Also, be stingy with personal information in your public profile. Strangers (and the social media behemoths themselves) don't need to know your gender, whether you're married, your birth date, or your location.

Check the privacy settings

I'm not sure how much good this does, since Big Tech is not known for keeping its privacy promises, but be sure to check the privacy settings in each platform (both on your browser and in their apps) to turn off advertising tracking, location tracking, and so on

Do this on a regular basis; I can't tell you how many times I returned to my privacy settings, on both social media and other sites, and discovered they'd magically changed back.

The Electronic Frontier Foundation put together a very, very detailed set of instructions for tightening up your privacy settings on Facebook and Instagram—which is

great because many of these settings are hidden in obscure places. When I went through the process for a friend I was shocked to see exactly what Facebook was tracking and the details they were sending to third parties.

Opt out of AI data collection

Do you want the social platforms to let AI bots scrape your data? Yeah, me neither. Make your preference known—typically in the platforms' Privacy & Security settings—or let Redact's premium (paid) service opt you out of 30+ platform's AI-powered data collection services.

If you use ChatGPT, the chatbot may have access to very private information. And there's always the threat that it will be leaked: In 2023, a tech issue exposed users' conversation histories.

Here's how to delete your data from ChatGPT:

1. Click the Profile icon in the top-right corner of the screen.
2. Select *Settings*.
3. Scroll down to the *Account* section and click *Clear History*.
4. Confirm by clicking *Clear History* in the pop-up window.

And you're done!

Make your website your home base with POSSE

In some careers, building an audience online is crucial; for example, artists, writers, and podcasters need to share their content to survive.

However, the social media platforms you depend on can kick you off, erase all your posts, or go out of business instantly and with no warning, taking your content and your audience with them. We saw, when Elon Musk bought Twitter—and later when TikTok went dark for a day—how quickly even an established social media platform can be destabilized.

Instead, why not share your thoughts, creations, and content on a platform you own?

One method to do this is called POSSE: Publish (on your) Own Site, Syndicate Elsewhere. With this strategy, you get to participate in social media while reclaiming some power from these exploitative digital platforms. No matter what happens to these platforms, your content, engagement, and followers will be safe because they will also live on your own site.

POSSE can be as simple as publishing posts on your own site and manually copy-pasting them into the various social platforms with a link back to your site. Or it can be as involved as setting up special tools to automatically syndicate your content to the platforms and "reverse syndicate" the comments and likes back to you.

The first step is to set up a website under your own domain. Don't know what website host to use? Wordpress lets you build a federated blog.

Once you have your website ready, take a look at these helpful resources to learn how to get set up for POSSE:

- POSSE (IndieWeb). This entry includes information on why you should go with the POSSE approach and has instructions on how to set it up. Warning: The instructions iare fairly technical.
- The poster's guide to the internet of the future (The Verge). A thorough article for lay people.
- Great article on #POSSE by @davidpierce.xyz (Tantek.com). This is a response to the Verge article above. At the end of the post, author Tantek Çelik lists many, many tools and resources to dive into as you set up your own POSSE website—like Brid.gy, a free tool that connects your site to various social media platforms.

- Çelik's front page is a good example of a POSSE site.
- POSSE: Publish on your Own Site, Syndicate Elsewhere - Hacker News (Y Combinator) This thread tackles some of the disadvantages of POSSE; for example, if you use this method to post on social media without having to be there yourself, you won't see your friends' posts. Some commenters offer solutions for various issues.

Moving to a POSSE approach may seem complicated, but it's no more difficult than learning the ever-changing ins and outs of each social media platform—from video orientation to post length to tagging. Once you get through the learning curve, the experience should become much more streamlined and intuitive.

The OPSEC Guide, published in February 2025, gets serious about social media protection—plus anonymous browsing, biometric-behavioral threats, and much more.

PART 5

DISENGAGE BY...RECLAIMING YOUR ATTENTION

Big Tech vies for our attention because they can turn it into profit. Pop-ups, audio and video ads, and every single thing on your smartphone are trying to distract you from living your life to get you to bow to their whims.

Consider this: Meta and Google are not nice companies that give away lots of free services. They are literally categorized as ad-tech companies. Their main business is selling your attention to advertisers.

According to Ezra Klein in a January 2025 podcast episode, “Attention is the world‘s most valuable resource.” When we store this resource for ourselves and dole it out wisely, not only do we shrink the attention thieves’ power...we live richer lives by focusing on what really matters to us.

CHAPTER 17

SLOW YOUR SURFING

Perhaps the best way to keep the internet from commandeering our attention is to use it as little as possible. To that end, before you hop online to look up a random fact, first consider: Do you really need this piece of information?

Looking back, I can't believe how many times I used to find myself reaching for my phone to look up the height of an actor in the movie I was watching, what year an historic event happened, or whether the crazy news a friend saw on Instagram is really true.

Whenever someone in my family had some inane question ("are sharks fish?"), we would joke, "Oh, if only we had a device with all the world's knowledge on it!"

Pulling out our phones or hopping onto our laptops to look up unnecessary information is so incredibly easy, we often don't realize the information is completely useless to us. Resisting this urge is a huge step toward disengaging.

CHAPTER 18

ANNIHILATE ADS

Online ads pop up, flash, and play audio and video to distract us from the goal we're trying to accomplish online. Free yourself of ads…and free up your attention for better things.

ANNIHILATE ADS BY…OPTING OUT OF ONLINE ADVERTISING NETWORKS

Online advertising networks are national trade groups that devise self-regulatory solutions to consumer issues online. In other words, they're groups of marketers and advertisers that give you cursory control over your data so they can avoid actual regulation.

Part of this weak effort is to let you opt out of a lot of their preference-based advertising. The process is clunky and they will warn you—over and over again—that if you opt out, the ads you see online will not be customized to you. (How out of touch can you get? I don't know a single person who complains that online ad companies know *too little* about them.)

Here's how to deny yourself the privilege of ads targeted to your behavior.

How to opt out of the Digital Advertising Alliance

Enter your email or phone number to control how advertisers collect data associated with that address or number. This won't affect ads you get via phone or email; the DAA's advertiser members only use this information only to identify you in order to exclude you from personalized ads online.

.

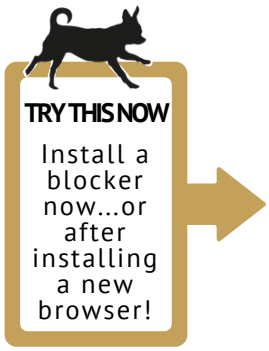
The site also lets you do a browser check to find out which of their member advertisers are customizing ads on your browser, and to opt out of any or all of them. I ran the check in the spring of 2023 and opted out of every one of all 118 advertisers. When I did it again in the fall of 2023, I discovered that a bunch of those advertisers were still serving personalized ads to my browser. So it's probably worth it to go through this process a couple of times per year.

How to opt out of the Network Advertising Initiative

Enter your email to opt out of member companies' browser-based advertising and matched advertising. There are also instructions for opting out of interest-based ads on various mobile devices and internet-connected TVs. (FYI, I discovered that if you try to opt out while using a VPN, you'll get an error on that page.)

ANNIHILATE ADS BY...BLOCKING THEM OUTRIGHT

Opting out of these networks doesn't stop ads—it only stops member companies from tracking you in order to



get rid of ads online altogether, you'll need to install an ad-blocking browser extension. These are a few popular ones:

- Adblock Plus (for Chrome, Firefox, Safari, Edge, Opera, and Android)
- AdBlock (for Chrome, Firefox, Edge, Safari, iOS, and Android)
- uBlock Origin (for Chrome, Firefox, Edge, and Opera)

Ad-blockers also prevent third parties from installing cookies on your device, so you reclaim your attention and your data all at once...for free!

Some of your favorite online content may be funded by advertising. You could always turn off your ad-blocker to allow ads from creators you want to support. (Some sites will display a pop-up asking you to support them by disabling your ad-blocker while on their site.)

CHAPTER 19

SAY SEE YA TO YOUR SMARTPHONE

Just 15 years ago, we managed to navigate the world without having to look at our phones 144 times per day—like we do now, according to PCMag. That's nine times per hour, or about once every seven minutes! Today we're completely reliant on our phones, pouring our life energy and attention into the very features and apps that suck up and share our data.

But...how can we find our way to a new friend's house without the GPS on our phone? How else can we get boarding passes, find a new restaurant, deposit checks, listen to audiobooks, join video chats, play music, tell the time, know whether to bring an umbrella, identify a bird, check our heart rate, or find out the name of the song playing at the local café?

Don't despair: Just as it was possible before, it's possible now. Not super easy, thanks to the way our phones have wormed their way into a position of such significance in our lives, but not as difficult as you might think.

OPTION 1: TRADE YOUR SMARTPHONE FOR A DUMB PHONE

I tried all the tricks of taking email off my phone and disabling the browser, but I'd instead find myself

checking the weather an unreasonable number of times, looking at photos (again), and checking my bank account over and over.

So when my smartphone died, instead of buying a new one, I opted for the LightPhone II—a small, privacy-oriented phone with a backlit black-and-white display that came with the bare minimum: phone, time, and text. You could use the online dashboard to add a few extras like a podcast player, music player, or map.

Incredibly, within just a couple weeks, I no longer felt the urge to check my phone. I could sit in the car, wait in line, or chill on my porch...without needing a gadget!

The bad news is, the main functions—texting and calling—were clunky, slow, and difficult. Part of my screen was unresponsive, and the phone would also turn itself off at random times. Despite the company's excellent customer service, I couldn't get it to work well enough that I felt safe being out and about with this phone as my only form of communication. The company was kind enough to offer me a refund even though it was after the return window.

That said, many, many people love their LightPhone, so perhaps I just got a bad one. If you like the idea, it's worth trying out, especially knowing that the company does have a return policy. The latest version, the LightPhone III, comes with a camera, fingerprint sensor, flashlight, and other features.

OPTION 2: COMPROMISE WITH A SEMI-SMART PHONE

While using the LightPhone II, I did have to endure some inconveniences. For example, I borrowed my partner's phone to deposit checks, used my laptop to make Venmo payments, and went to the wall thermostat to see the temperature outside. When a business required customers to scan a QR code for service, I marched up to the front desk and asked for an alternative.

Not willing or able to sacrifice Uber, the weather, or other apps? Some LightPhone users also keep an old smartphone and swap in the SIM card when they need to use it.

If you want a distraction-free phone but the inconveniences of a true dumb phone are a deal-breaker for you, try one of these semi-smart phones or privacy-forward smart phones.

- WisePhone II looks like an actual smartphone and includes music, calculator, maps, phone, messages, camera, flashlight, photos, clock, notes, a calendar, and more—but no social media apps, browser, or app store. The company bills itself as a conservative and religious business, if that matters to you either way. Their privacy policy states they will not sell, rent, or provide your information to any third parties for marketing purposes.

- The Ghost Phone looks similar to WisePhone II and has many of the same features. In addition, it has its own small app store, and many other apps can be sideloaded to the phone—but browsers and social media apps will be blocked. The Ghost Phone Pro runs on an Android-based operating system, and while it purports to reduce distraction, I couldn't find any claims to privacy.
- The Fairphone with 5/e/OS is "a fully 'deGoogled' version of Android—built on open-source tech." It comes preloaded with apps like email, calendar, chat, web browsing, and weather. The operating system also works with all Android apps while keeping your data private.

Not all phones are compatible with all carriers; for example, my LightPhone didn't work with Visible, my carrier at the time. Check the phone's website to see if you can stick with your current carrier.

For more brands to consider, search for "distraction-free phone." (Not on Google, though! More on search engines later.) Or, if you're not looking for a lot of features, look for an old-school flip phone like the Nokia 2780 Flip.

OPTION 3: INSTALL A PRIVACY-FIRST OPERATING SYSTEM

For those more concerned about privacy than distraction, here's another possibility: Buy a used Pixel phone and install GrapheneOS, a free, privacy-oriented operating system for Android phones. GrapheneOS is an open source non-profit that also develops secure and private apps and services—so you can keep your data out of Big Tech's hands without missing out on, say, a camera or a browser.

I finally did this, and I'm so glad I did. When my kid's iPhone finally died, I gave them mine and ordered a refurbished Pixel 7a for $200 from Gazelle. After downloading my contacts to my laptop and uploading my photos to Proton Drive, I went to the Graphene site and followed their instructions. There were a few user-error glitches at the start, but then the process was fast and smooth.

The Graphene operating system is clean and easy to use, and comes with basic apps. For other apps, download from Google Play. GrapheneOS has a special "compatibility layer" that lets you use Google Play apps without forfeiting your privacy.

Whatever kind of phone you have, consider getting a cover for your front-facing camera. (And pick up one for your laptop, while you're at it.) These gadgets cost only a few bucks, and they not only thwart hackers gaining access to your camera through malware, phishing attacks, and other bad-guy tactics—they also save you from potentially embarrassing situations when you forget your camera is turned on before or after a video call.

CHAPTER 20

GHOST CORPORATE NEWS

Remember earlier when I said Big Tech—and the billionaires that own these companies—are shaping the way we see the world? That's because some of them actually own the news.

In September 2024, Pew Research Center Reported, "Overall, just over half of U.S. adults (54%) say they at least sometimes get news from social media, up slightly compared with the last few years."

I don't know how many people turn to which social sites, but at the very least this means millions of people are taking in news on sites controlled by Mark Zuckerburg and Elon Musk. Then we have the Washington Post, which is owned by Amazon founder Jeff Bezos.

The rest of the media industry is just as concentrated. According to Wikipedia:

> In 1984, fifty independent media companies owned the majority of media interests within the United States. By 2011, 90% of the United States's media was controlled by six media conglomerates: GE/Comcast (NBC, Universal), News Corp (Fox News, Wall Street Journal, New York Post), Disney (ABC, ESPN, Pixar), Viacom (MTV, BET,

Paramount Pictures), Time Warner (CNN, HBO, Warner Bros.), and CBS (Showtime, NFL.com).

A lot of these are the major news networks millions of us turn to every day. They control what we know and what we see, while selling our eyeballs to advertisers.

Why not take some of the power from corporate-owned, ad-supported media—not to mention privacy-invading social media—and give it to reader-supported independent media instead? You can read many of them for free, or support them for extra perks like unlimited articles. Some subscriptions cost under a dollar per month.

Trustworthy Media offers a list of independent media outlets; it's not at all comprehensive but is a good start. If you're concerned about an outlet's political bias, check it at AllSides. You'll find that the majority of independent media leans left, but center and right-leaning outlets exist as well.

I personally have cancelled my New York Times subscription and now support Lever News, The Guardian, and Ground.News with paid subscriptions. If you already have a paid subscription to a mainstream news outlet, you'll drain a little power from our corporate overlords—and possibly save your sanity—by moving your money over to an independent one.

PART 6

DISENGAGE BY...QUITTING THE BIG 4

Hopefully, the actions you've taken to disengage so far have honed your wits for the biggest challenge of all: quitting Google, Amazon, Apple, and Microsoft—the biggest of Big Tech. (It's actually a Big 5, but we covered Meta/Facebook earlier.)

These are the companies that use their market power to lock us into their products, kill off competitors, assault us with ads, mistreat creators, and extract our data for corporate profit.

These are the corporations whose massive privacy violations have turned us from living, breathing humans into dollar signs and data points.

And they're the businesses with the dollars to buy our country right out from under us. Recall that CEOs from three of these four companies bent the knee at the President's inauguration. It's not clear if Microsoft's CEO was there, but the company did donate $1 million to the inaugural fund.

In this section of the book, I'll offer a quick critique of each of these surveillance capitalist companies—and some solid alternatives.

CHAPTER 21

SAY GOODBYE TO GOOGLE

Google's free products are hard to beat! Gmail, Google Drive, YouTube, Google Photos, Google News, the Chrome browser, and the list goes on.

However, Google is also one of the world's most ruthless harvesters of your personal data—which it doesn't adequately protect, seeing as how it's exposed the personal info of hundreds of thousands of people.

The product Google is best known for, Search, isn't all that great: As the biggest server of online ads, the company prioritizes paid search results over what you actually want to find.lvii Scammers manipulate Google's algorithms to create junk sites that rank high in the search engine, ripping off both visitors and advertisers.

Then there's the monopoly issue. In September 2023, the U.S. launched an antitrust lawsuit against Google. "The Justice Department's case hinges on claims that Google illegally orchestrated its business dealings, so that it's the first search engine people see when they turn on their phones and web browsers," reports NPR. "The government says Google's goal was to stomp out competition."

In February 2025, Google removed from its “AI Principles” its promise to not use AI for weapons or surveillance.

All this and (much) more is why it makes sense to explore the big world outside of Google products. This can be a difficult endeavor at the beginning, but once you move to new platforms, they’ll become as much a part of your everyday life as Google once was. After some up-front effort, you don’t need to think about it ever again. (And I know because I’ve done it myself.)

For more alternatives to Google and all Big Tech offerings, visit ethical.net, a not-for-profit project building a collaborative, online directory of ethical companies of all kinds.

If you’d like to kick Google to the curb, Nord VPN provides a list of Google alternatives, many of which are free or cheap.

I researched and tested some of NordVPN’s suggested replacements as I went about getting rid of Google products in my own life. Here’s what I ended up using and how well these replacements worked. Like Google products, many of these alternatives are free but offer more space, features, and so on for a fee.

EMAIL: GMAIL → PROTON MAIL

I chose Proton, a privacy-first email provider that also offers a calendar, password manager, VPN, masked emails, and more. Get an email address for free, or upgrade for more addresses, the ability to use your own domain, and other features.

I've been very happy with Proton except I find their email search to be slow and annoying. However, that's the upshot of extra privacy. Google provides the fast searches they do because they have access to your content, giving them a perpetual searchable index of your data.

Changing over was a long-term process. Here's how I handled it:

- Deleted all Gmail accounts except for my main one, as I had different addresses for different purposes.
- Set up the main Gmail account to forward to the new Proton account.
- Set up this automated response on Gmail:

> **Subject Line:** This email address is no longer being monitored
>
> **Body:** Hi! This email address is no longer being monitored. If you know me and didn't get my new address, please text me. Otherwise, you can contact me through my website, [URL]. Thanks!

- On Proton, created two email addresses: one for friends and family, and a second one for businesses and organizations I trust.
- Emailed my friends and family to give them my new (main) email address.
- Changed over all important accounts to use the second email address. (Less important accounts, such my local supermarket, get masked emails; see Chapter 8: Escape Email Tracking for more on masked email addresses.)
- Changed the email address on my website, my downloadable content, etc. to a masked address.

For the first few weeks, I occasionally caught forwarded emails from people and businesses I neglected to alert to the change, and I switched them over to one of the new addresses. At some point, I started getting nothing but spam at my main Gmail address.

Once I moved all my files out of Google Drive (more on that below), I took a deep breath and deleted my main Google account. It felt so good!

Discover other free or cheap private email providers in Chapter 7: Surf in Secret.

SEARCH: GOOGLE SEARCH → KAGI, DUCKDUCKGO, OR SIMPLESEARCH

Rather than using Google Search, I use Kagi Search. You get 100 free searches with their trial, and believe me when I say you'll want to upgrade. I now pay about $12.50 per month for unlimited searches for both my partner and myself, and it's worth every cent.

Since Kagi is not ad-supported, you don't see ads. Your searches and other data are private. You can raise or lower websites rankings—for example, if you want to see more results from WebMD or fewer from WikiHow. Kagi also lets you create "lenses" for more personalized results. And the search results are just *better*: no AI spam, no junk.

Here's how to change your default search engine to Kagi.

If Kagi's price is too steep, check out the privacy-oriented DuckDuckGo, which I used for several months before switching to Kagi. It's free, but because it doesn't track or collect your info, search results are not personalized or hyper-targeted. I consider this a good thing, as I don't *want* to be confined to a little bubble when it comes to what information I see. It took a few weeks to get used to DuckDuckGo, but after that I didn't even give it a second thought.

To change the default search engine to DuckDuckGo in your computer's browser, simply click on the magnifying

glass in the search bar, click on *Change Search Settings* in the dropdown menu, and choose DuckDuckGo under the Default Search Engine section. Follow these instructions for iOS; these are the steps for Android.

Don't want to pay for Kagi, and/or can't do without the ease and personalization of Google Search? Simple Search is an extension for Firefox and Chrome that highlights the *actual search results* provided by Google or Bing, cutting out all the paid search ads, info boxes, etc.

Using Simple Search doesn't mean these search engines can't track you, collect your data, or serve up personalized ads—it just means *you* don't see those ads, which throws a tiny bit of sand into Google's money-making gears.

CALENDAR: GOOGLE CALENDAR → PROTON CALENDAR

A Proton account includes Proton Calendar, which works pretty much the same as Google Calendar. The disadvantage is that while you can *share* and *view* events between the two platforms, you can't *edit* events created in the other platform.

PHOTOS: GOOGLE PHOTOS → ENTE OR PROTON DRIVE

I first replaced Google Photos with an app called Ente. This paid platform lets you organize and store photos both in the app and online. The developers are big on privacy, and I found it to be worth the money.

But then I discovered that the Proton Drive app automatically back ups and encrypt your photos. The back-up is a bit slow, but it's fine—especially considering I was already paying for a subscription.

NEWS: GOOGLE NEWS → GROUND.NEWS

Ground.News "process[es] nearly 60,000 news articles from over 50,000 different news sources. Articles from different outlets covering the same event are merged into a single summary, making it possible to get multiple perspectives in one place."

I think of it as the non-Google Google News, with the extra perk that the service marks each story with Bias and Factuality ratings.

The site is free, but a paid subscription gets you more features. Subscriptions start at $9.99 per year. Yes, per *year*!

BROWSER: GOOGLE CHROME → FIREFOX OR A PRIVACY BROWSER

I chose Mozilla's Firefox browser in place of Google Chrome, and have been happy with it. Mozilla is a non-profit stating, "Individuals' security and privacy [...] are fundamental and must not be treated as optional."

The only catch is, you need to "harden" Firefox by setting the privacy restrictions and using a tracking blocker like Ublock Origin.

As I write this, there has been some noise about Firefox's new privacy policy; it does look like people are not reading it fully or are misinterpreting it, but if this makes you worried, you can avoid it. In this case, there are privacy-first browsers you might like to try. Some to think about include Mullvad, Epic Privacy Browser, Orion browser, and Librewolf.

Whichever you choose, install it before changing it to your default browser.

How to change the default web browser on iOS

1. Go to *Settings*.
2. Select *Apps*.
3. Tap *Default Apps* at the top of the list of your apps.
4. Tap a feature to change your default setting to a different app.
5. After choosing a new default app, you might have to follow additional onscreen steps.

How to change the default web browser on MacOS

1. From the Apple menu in the corner of your screen, choose *System Settings*.
2. Click *Desktop & Dock* in the sidebar.
3. Scroll down on the right and choose a web browser from the *Default web browser* menu.

How to change the default web browser on Android

1. Open the *Settings* menu.
2. Select *Apps* or *Applications*.
3. Tap the three-dot menu icon in the top-right corner and choose *Default apps*.
4. Tap *Browser app* or *Browser*.
5. Select the browser you want to set as the default.
6. If prompted, select *Set as default* or a similar option to confirm.

How to change the default web browser on Windows 11

1. Press the Windows key or click the Search Bar and type *Default Apps*.
2. Click *Default Apps*.
3. In the search bar under *Set Defaults for Applications*, type the new browser name and click on it.
4. Click *Set Default*.

You did it! Now, when you click on a link in, say, a text, it will open in the correct browser. Be sure to set the new browser as default on your desktop computer, phone, and other devices.

Brave bills itself as a private browser, but according to AndroidPolice:

“Brave Browser is undeniably a commercial product first, and a privacy-centric web browser second. While the browser does have quite a few improvements to privacy compared to stock Chrome, it's designed to promote the use of a cryptocurrency (BAT) that Brave itself owns, and it has a referral program that pays browser users by how many people they can get to download Brave. Now the browser has been caught injecting its own affiliate codes into web addresses for popular cryptocurrency trading websites.”

I read in other places that the affiliate code snafu was an honest mistake. However, if you lean left, know that the CEO has questionable ethics, and Peter Thiel’s Founders Fund was a major backer of Brave.

So considering there are so many other privacy browsers, if these facts worry you, just choose another one.

MAPS: GOOGLE MAPS → KAGI MAPS, OSMAND, HERE WEGO, OR PAPER MAPS

I use Kagi maps, which is available for subscribers. According to their website, "Unlike other competing Map services that track your location to serve you ads, Kagi does not track or store your search history or location data."

Looking for free maps? Try OsmAnd, which NordVPN calls "one of the leading privacy-oriented Google Maps alternatives" or HERE WeGo, which "falls under GDPR rules and regulations, so you can be sure that your data is in good hands." I tested out HERE WeGo and it worked just as well as Google or Apple maps.

And for the ultimate in privacy, don't forget that paper maps still exist. We keep a road atlas in each car for emergencies.

The popular Waze app was acquired by Google over a decade ago.

VIDEO: YOUTUBE → NEBULA, PEERTUBE, OR YOUTUBE (!!)

Some of the same creators who post on YouTube also post on Nebula, "a place for experimentation and

exploration, with exclusive originals, bonus content, and no ads in sight." Half of your subscription fees ($6 per month or $60 per year) go to the creators.

If you prefer to watch for free, PeerTube is a federated social platform on a mission to provide an alternative to Big Tech. According to the website, "With PeerTube, no more opaque algorithms or obscure moderation policies! PeerTube platforms you visit are built, managed and moderated by their owners. PeerTube allows platforms to be connected to each other, creating a big network of platforms that are both autonomous and interconnected."

I searched for "music," "gardening," and "video games" to see what I could find. As of this writing, PeerTube is hosting 900 music channels, 10 gardening channels, and 4,200 video game channels. It's nothing compared to YouTube, but if more people like us use it, it will keep growing.

Can't find what you need on Nebula or PeerTube? Here's some good news: You don't need to be logged into Google/YouTube in order to watch videos. You'll lose out on some features—such as subscribing, liking, and commenting on videos—but it's a small price to pay if you prefer to be slightly more anonymous.

(I say "slightly more" because I doubt you're invisible to Google just because you're not logged in. But again, every little resistance helps!)

LAPTOP: GOOGLE CHROMEBOOK → LENOVO OR DELL

If you want to steer clear of both Google and Apple, many cybersecurity experts are recommending Lenovo and Dell laptops as secure alternatives.

Whatever laptop you opt for, consider switching your operating system to Linux: a free, open source operating system that gives you more control over your privacy. There are many tutorials online for switching over your current laptop, and dedicated Linux machines are also available. Michael Bazzell goes into detail on the options in his book *Extreme Privacy*.

CLOUD DOCUMENT EDITOR: GOOGLE DOCS → ZOHO OFFICE, PROTON DOCS, OR CRYPTPAD

Zoho Office is one of Google Docs' biggest competitors, because it includes a whole suite of tools like editing, chat, and an offline app. The platform also lets you upload different types of documents and even edit PDFs. On top of all that, it has a clear and reasonable privacy policy.

Zoho Office's Writer, Notebook, Sheet, and Show products duplicate Google's popular office products and are free

for individuals; access all of these through Zoho's Workspace, which offers 5GB of storage per user with up to five users, and a 25MB attachment limit.

I'm also thrilled that Proton now offers a cloud-based document editor as part of Proton Drive. It doesn't have all the features of Google Docs (yet), but it keeps adding new ones. I now use Proton Docs for word processing documents and Zoho for spreadsheets.

Finally, I discovered and tested out CryptPad, "the end-to-end encrypted and open-source collaboration suite." CryptPad lets users create and collaborate on text documents, worksheets, forms, and more.

I found CryptPad through PRISM Break, which has lists of suggested alternatives to global data surveillance programs. The website states, "Help make mass surveillance of entire populations uneconomical! We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services."

On this site you'll find safer apps for email, file sharing, financial tools, productivity tools, social media, and much, much more—for both mobile devices and computers.

CLOUD STORAGE: GOOGLE DRIVE → PROTON DRIVE

I originally chose Box.com as my new cloud storage solution because it allows users to collaborate on and share documents; however, when I attempted to switch over to Box, I was continually frustrated at how slow and inconvenient it was.

First, there was no easy way to automatically transfer the contents of your Google Drive. I tried various methods, and finally resigned myself to downloading all my folders from Google Drive and then uploading them into Box Drive.

Second, I discovered if you try to upload folders that contain subfolders, many of the subfolders' contents don't transfer over. So my next task was to upload the individual subfolders one by one. This entire process took several days, on and off.

Third, the editing and sharing of files is very clunky. In order to share a file, the recipient needs to have a Box account—which makes sense, but who wants to go to that much effort just to collaborate with little old me? And in order to open and work on files in Box, you have to use third-party apps like Microsoft Word, which defeats the purpose of choosing a privacy-oriented drive.

Finally, I had the terrifying experience of losing thousands of files when I tried to reorganize my drive.

Thank goodness I hadn't deleted the files from Google Drive yet, so I gave up, canceled my Box subscription, and went crawling back to Google.

Later, I moved to Proton Drive for storage. I like it, with the exception of their search: They only allow you to search by title and not by content. However, this is because, unlike Google, Proton doesn't have access to your documents. That's part of what makes it private!

How to stop paying Google for storage

Until I had the chance to move to Proton Drive, I cleared out my Drive files from many, many gigs to under 15 GB. This not only let me stop paying for Drive—thereby withdrawing my dollars from Google—but also helped me minimize the amount of my content Google had access to.

If you'd like to reduce your Google storage to "free" levels, here are some tricks I used. (Also, if you ever decide to move to another cloud storage service, you won't be paying for storage you don't need.)

Step 1: Decide what you need

"Storage is cheap!" we say as we upload masses of files. And now, if you're like I was, you have hundreds or thousands of files in Drive you don't really need. For example, I had saved *every single file* from the last 25+ years of my career.

What do you really need to have hanging around in

Google Drive? For me, it was important personal projects, the last two years' worth of client work, and projects I was working on right then.

Do you really need to hang on to 10-year-old resumes, background files from work projects long past, and every draft of your novel? Be ruthless in your choices.

Step 2: Delete large files

In Drive, click *Storage* and sort the files by size, from biggest to smallest. Are there any large videos, images, or other files that you don't need sucking up a lot of space? Trash them.

To declutter even more, click *Storage* and then *Clean Up Space* to see files in Drive, Google Photos, and Gmail that Google recommends you delete.

Step 3: Ditch duplicate files

Duplicate files can be a big culprit in hogging your storage space. If you're on Android, Google provides an easy solution:

1. Open *Files by Google*.
2. Tap the menu, then *Clean*.
3. On the *Duplicate files* card, tap *Select files*.
4. Select the files you want to delete. The original file is marked with an *Original* badge.
5. Click *Move # file(s) to Trash*.
6. On the pop-up, tap *Move # file(s) to Trash*.

Step 4: Manually trash unneeded files

Now that you know which files are crucial and which are not, delete all the deadwood. This is a very satisfying task.

Step 5: Transfer old (but important) files to a different service

If you have lots of files you want to keep, but you no longer need to share or collaborate on, transfer them to a privacy-forward Google Drive alternative such as Proton Drive or *Sia* (for the more tech-savvy among us).

Step 6: Move files to an external hard drive

Finally, I copied all the files from Proton Drive to an external hard drive; the most important of these files I also keep on my laptop. I store the hard drive in a fireproof safe and upload new files to it monthly.

Step 7: Empty the trash

Drive does this automatically every 30 days, but in the meantime your trashed files may be taking up a lot of space.

More ways to disengage from Google

You didn't really think you were done, did you? Here are two more ways to keep Google from tracking your every move.

1. Turn off Google tracking

If quitting without Google products is a no-go for you, visit the company's Data & Privacy page to choose who is allowed to see your personal information, tell Google not to track your browsing history, turn off personalized ads, and more. Also disable Google's tracking on your Android devices, Nest thermostat, and other Google gadgets.

2. Opt out of Google Analytics

Google Analytics is a web analytics service that tracks and reports website traffic. Website owners can look at their Google Analytics dashboard to find out their visitors' IP addresses, locations, devices, visit lengths, browser settings, and more. The platform does this by using tags on the websites that run in visitors' web browsers, collecting their data and sending it to Google's data collection servers.

If you want to prevent Google Analytics from using your data, take advantage of the Google Analytics opt-out browser add-on for Chrome, Firefox, Safari, and Edge browsers.

CHAPTER 22

SAY AU REVOIR TO AMAZON

Amazon lures and then locks in consumers with low prices, which it accomplishes by squeezing its producers—creating an environment where the producers have to squeeze their employees in order to keep prices low.

Once it has a critical mass of consumers, Amazon cuts out the product providers altogether by copying their products, enticing creators to work directly with Amazon, and using its commercial power to bully, buy up, or kill other businesses.

For example, when the founders of Diapers.com wouldn't sell, Amazon started offering deep discounts and free shipping on diapers, dropping its price every time Diapers.com did until the smaller business gave in. Once Amazon bought Diapers.com, it closed the company down.

This leaves us with few choices for where to purchase crucial products, stripped-out common spaces where local companies have been run out of business, and no limits on how badly Amazon can treat its customers and employees. Not only that, but people have been complaining that the products they're receiving from

Amazon these days are either of shoddy quality or straight-up counterfeits. I'm not talking about luxury items here, but basic items like face lotion and board games.

"But the prices are so low!" we say. Not so: Even Amazon's premise of ultra-low prices is a sham. According to Cory Doctorow in his Plura-list newsletter:

> If you trust Amazon search to find you the best product and click that first link, you will pay a 29% premium for that item. If you expand your selection to [...] the first four items, which are often all that's visible without scrolling—you'll pay an average of 25% more. That top row accounts for 64% of Amazon's clicks. On average, the best deal on Amazon is found in the seventeenth slot in the search results. Seventeen!

For some of us, Amazon is essential; for example, people who live in rural areas or who don't have reliable transportation benefit from fast delivery of products they need. But others have the luxury of considering Amazon products wants instead of needs.

HOW TO STOP SHOPPING ON AMAZON

If you're among the latter, here's how to free yourself from Amazon shopping.

Stop Shopping at Amazon by…resetting your expectations

Amazon has trained us to expect near-instant delivery of everything we want. Decide your coffee mugs are looking shabby? Just one click and a sparkling new set will be delivered to your home today.

Retrain yourself to wait a little longer for what you want. A smaller shop may have slower shipping, but that's OK—learn to look ahead instead of racing to Amazon whenever you suddenly want something. You also may have to wait a few days until you have a chance to visit a brick-and-mortar store for that plant stand or battery recharger; this will give you the time to consider whether you really need one in the first place, or whether you might be able to find one through your local Buy Nothing group.

Stop Shopping at Amazon by…canceling Prime

The next step is to cancel your Prime subscription. (Remember this means you'll also lose access to Prime Video movies and TV shows.) Think about it: Outside of a few perks you probably don't need, your Prime subscription is essentially *you pre-paying for your own shipping*. (You're not spending $139 for free shipping, you're paying $139 for shipping.)

This means you're not giving up much in terms of savings when you quit Prime. "Recall that Amazon

already comps shipping on orders over $25, so a potential Prime purchaser has to evaluate whether they'll place enough sub-$25 orders in the coming year to justify the price—and also factor in the fact that Prime items are often more expensive on a per-unit basis than their non-Prime equivalents," writes Doctorow. [The minimum has since been raised to $35.]

Stop Shopping at Amazon by...knowing your enemy

Amazon isn't just Amazon. They also own companies like:

- Zappos
- Goodreads
- PillPack, a pharmacy
- One Medical
- Whole Foods
- Ring LLC (the smart doorbell company)
- Twitch, the streaming video platform for gamers
- Wondery, a podcast publisher and network
- iRobot, makers of the Roomba, which Bloomberg calls "a data collection machine that comes with a vacuum."
- Audible, the audiobook store

Here's an infographic that names every business owned by Amazon as of June 2022. If you know a business is owned by Amazon...look elsewhere.

Stop Shopping at Amazon by…looking around town

Explore your downtown and other local shopping centers. You may be surprised at what you find. My town has a sew-n-vac store, a woodworking shop, and other gems I never noticed before.

Your neighbors may also be good sources of products you want; for example, I have neighbors who sell cakes, handmade signs, and more.

Stop Shopping at Amazon by…going direct to the source

Many shops sell their wares both on Amazon and on their own websites. (Sadly, Amazon prohibits sellers from charging lower prices off its platform, which raises prices *everywhere*.)

See something you want on Amazon? Go directly to the manufacturer's website. I've been able to buy specialty vitamins, jar labels, bakery boxes, vacuum parts, specialty flour, and more right from the producer.

I may give up free shipping, in which case I sometimes wait until I need enough from the seller to reach the free shipping level. (Also recall that Prime shipping isn't really free!)

Stop Shopping at Amazon by…going where the pros go

Another idea is to buy in bulk from specialty shops. I've bought five-pound bags of sesame seeds from BulkFoods.com for less than $25, including shipping. (Amazon does not beat this price, even with "free" shipping.)

From WebstaurantStore I've bought cases of coffee flavoring syrup for $6.39 per bottle plus shipping. (The cheapest on Amazon is $14 per bottle. That's more than twice as much!)

WebstarauntStore also offers dishware, coffee makers, food storage supplies, baking ingredients, condiments, table décor, and much more. You don't have to buy multiples of everything, but it's cheaper if you do; for example, one 20 oz French coffee press is $8.99, but they're only $7.99 each in lots of 12.

If you need a lot of something—or can split it with friends—bulk and wholesale shops like these are the places to go.

Stop Shopping at Amazon by…looking for alternatives

If you're still on social media at this point, ask around for suggestions on where else to buy that missing keyboard key, set of food storage containers, or baby bib.

Rolling Stone ran an article in December 2024 on 13 Amazon alternatives for your holiday shopping. Here are the best from their list:

- REI
- Thrive Market
- Hive
- Grove
- Huckleberry
- Public Goods
- World Market
- Chewy
- Uncommon Goods

Visit the article for more details on (and links for) each of these shops.

Stop Shopping at Amazon by...getting creative

Whenever you need something you know you can't find locally, see if it's available from a smaller company online. When I wanted a unique gift for a friend who is an incredible host, I found handmade serving trays created from recycled wine bottles at Uncommon Goods. I've also bought memorial trees, homemade brownies, and other goodies sold by smaller companies online.

Stop Shopping at Amazon by...visiting a warehouse store

Sometimes we just want to buy socks, shampoo, or AA batteries and don't want to search all over town for them. Costco is my go-to for times like this.

I used to recommend big-box stores like Target and Walmart, but they're on my no-go list now due to their business practices, plus Target's quick decision to demolish its DEI initiatives in January 2025.

Costco has committed to keeping its DEI program, and as of this writing they pay entry-level workers $20 per hour and higher-level workers $30+ per hour. According to NPR, "The chain's pay is among the highest in retail, which has helped Costco maintain a lower turnover rate than most rivals."

Stop Shopping at Amazon by...getting what you need for free

Freecycle, Craigslist, and your local Buy Nothing group (which also has an app) are places where people give away everything from moving boxes to furniture to appliances. On my local Freecycle I found, among other items, a soft-sided dog crate, a working refrigerator, and a landscape painting. Many people offer items when they're in declutter mode and don't want to bother listing a bunch of things for sale.

HOW TO STOP BUYING BOOKS ON AMAZON

Amazon may be best known for its bookstore, brimming with not only print books but also e-books and audiobooks (through Audible). Amazon sells titles from big-name authors and self-published writers alike.

Sadly, though, the company is also harmful to the book publishing industry, squeezing creators and publishers while making it difficult for them to sell elsewhere.

If you're tired enough of Amazon's shenanigans to kick them to the curb, there are ways to keep reading without Amazon, Kindle, or Audible.

Use another e-reader

If you use a Kindle e-reader, you're stuck buying e-books from Amazon. That's because Amazon supports only its proprietary AZW e-book files, and doesn't allow you to load files in other formats.

Let me just repeat that you *bought and own* a reading device, but *have no control over what you can read on it*. Amazon has made this seem normal, but it's not.

All is not lost! You could always keep your Kindle books on your Kindle and then start a new collection on another e-reader. It may not be the very most convenient option if you like to reread books frequently, but if you're mostly "once and done," you won't need to pull out the Kindle too often.

Ready to find a new e-reader? Here are some Kindle alternatives that let you read a variety of file formats.

- Kobo supports EPUB, EPUB2, EPUB3, PDF, FlePub, MOBI, JPEG, GIF, PNG, BMP, TIFF, TXT, HTML, RTF, and CBZ and CBR Comic Book formats.
- Onyx Boox e-readers support these file formats: TXT, HTML, RTF, FB2, FB2.zip, FB3, DOC, DOCX, PRC, MOBI, CHM, PDB, EPUB, JPG, PNG, GIF, BMP, PDF, DjVu, MP3, WAV, CBR, and CBZ. Check out their feature-comparison chart.
- NOOK e-readers from Barnes & Noble support EPUB and PDF file formats. Some also support the CBZ comic book format. This means they support ebooks not just from Barnes & Noble, but also from other online booksellers.

Within these brands, you'll find everything from e-ink devices similar to the Kindle Paperwhite to backlit e-readers, and even color e-ink screens.

They come in different sizes, typically have a long battery life, and some of them let you mark up books with a stylus or your fingers. Apps that let you read across devices, speakers for audiobooks, and the ability to borrow from libraries make many of these e-readers very convenient.

A few are even water resistant or waterproof, for those of us who like to read in the bath.

Once you have an e-reader that lets you read all kinds of files, it opens up a whole world of small and independent online booksellers. Try sites like:

- Bookshop.org is known for selling print books with proceeds going to your favorite independent bookstore. In February 2025 they developed a platform for independent shops to sell e-books. Right now you can read e-books only online or in the Bookshop.org app, but according to their website, "We are working with Kobo to support Kobo devices later [in 2025]."
- Smashwords, which offers nearly one million original e-books, including about 100,000 free ones each day. These are mainly Digital Rights Management-free EPUB files, which means you won't see many of the traditionally published books that you'll find in bookstores.
- Project Gutenberg, which mostly publishes works in the public domain.
- e-books.com, one of the world's oldest and largest sellers of e-books. Here is a list of supported e-readers. Or read their e-books on their app, or on your computer using the free Adobe Digital Editions software.
- Author and publisher sites. Some sell DRM-free books that work on an array of devices. For example, Tor Books and Baen are publishers to look at for sci-fi and fantasy. Author Cory Doctorow sells all his e-books and audiobooks DRM-free.

Once you get used to a new way of sourcing and reading e-books, you'll never want to give your hard-earned book money to Amazon again.

Abandon Audible

Not only is Audible an Amazon company…it doesn't let libraries lend its Audible Exclusive titles, limiting access to some major books. Here are some better options.

- Libro.fm provides access to audiobooks from over 2,500 partner bookstores. You get to pick a local bookstore to support with your purchases.
- Everand charges $11.99 per month for access to audiobooks as well as e-books, magazines, newspapers, and more—adding up to millions of works. There are monthly limits for certain e-books and audiobooks, but otherwise it's an all-you-can-read situation.
- Chirp lets you escape subscription fees; after all, why is it considered a given that we have to subscribe for audiobook access while we can purchase e-books and physical books individually? Chirp has limited-time deals on select audiobooks plus low everyday pricing for everything else.
- LibriVox offers free audiobooks of public domain works read by volunteers from all over the world.

With alternatives like these, you won't lose much (or anything) by ousting Audible.

Shop at independent bookstores

You think they're gone, but they're not. Scrappy brick-and-mortar independent bookstores have popped up in many cities in defiance of Amazon and big-box bookstores. (Not to mention, we do still have big-box booksellers like Barnes & Noble.)

A search on Indiebound found eight independent bookstores within 20 miles of my zip code. Just enter your city or zip to see what's available near you. Some of them even ship books. The one I shop at has excellent customer service, shipping, and a loyalty program offering a generous discount.

If you prefer to buy your physical books online, try Powell's Books, the world's largest independent bookseller, or Bookshop.org, where every purchase on the site financially supports an independent bookstore of your choice.

Another shop to consider is Thriftbooks, an online store that specializes in used books. They get their books in bulk from libraries, thrift stores, and other sources.

Go to the library

Many libraries lend not just print books, but e-books and audiobooks as well. The number and variety of these formats varies depending on how large your library is and where it's located.

The easiest way to find and borrow e-books and audiobooks is to download the Libby app. Your library's website may also have a catalog; when you find a book you'd like to borrow, check the book's description page to see which formats it's available in.

CHAPTER 23

SAY ARRIVEDERCI TO APPLE

You may divide the world into “Mac people” and “PC people,” but that’s because Apple and Microsoft use monopolistic practices to make their systems and applications seem like the default. This excerpt from an NPR overview of a 2020 House Democrat report says it all:

> The report says Apple exerts "monopoly power" in the mobile app store market by favoring its own apps and disadvantaging rivals.
>
> That dominance hurts innovation and increases prices and choices for consumers, House investigators found. Apple, along with Google in its Google Play store, leaves developers with little choice for reaching consumers, the report says, adding that the arrangement leaves developers at the whims of the "arbitrary" enforcement of Apple's app guidelines.
>
> The report found that the controversial 30% commission levied by Apple and Google has resulted in price increases on consumers. Investigators say that Apple generated billions of dollars in profit from the fees, despite costing less than $100 million to operate.

Not only that, Apple has been accused of violating labor laws—and while the company touts its privacy practices,

a security researcher and developer claimed Apple apps collect and send data even if you declined to give consent for them to do so.

More recently, according to Forbes.com, Apple "has been secretly working with SpaceX and T-Mobile US Inc. to add support for the Starlink network in its latest iPhone software, providing an alternative to the company's in-house satellite-communication service." If you're one of those people who prefer not to give money to Elon Musk, then this is more incentive for you to avoid Apple products.

Finally, in February 2025, Apple said it will remove Advanced Data Protection for UK customers after the government demanded access to user data stored in iCloud. Who's to say it won't happen elsewhere?

To be fair, Apple is defending its DEI program—but seeing as how CEO Tim Cook was among those kissing the ring at the President's inauguration, I count Apple as one of the tech giants looking to take over our politics, communities, and individual lives.

Let's dive into some ideas for escaping the Apple ecosystem.

GO BACK TO THE PAST

First, use the tips from earlier chapters to disengage from Apple:

- See Chapter 21: Say Goodbye To Google for privacy-forward replacements for iCloud storage, iCloud mail, Apple Photos, and other products.
- See Chapter 19: Say See Ya To Your Smartphone for info on how to strengthen your privacy in phone apps...plus ideas for how to scrap your smartphone altogether.

Then, look to these alternatives to Apple software, music, and podcasts.

OPERATING SYSTEM: MAC → LINUX

If you feel up for the challenge, a Vice article on how to quit Big Tech recommends installing Linux on your Mac and replacing Mac's native applications with Linux equivalents. There are many free, open-source alternatives to various popular software programs that work with Linux.

STREAMING MUSIC: APPLE MUSIC → RESONATE, SOUNDCLOUD OR TIDAL

Want to abandon Apple music? Go one better by choosing an artist-friendly alternative that pays decent royalties to creators. These competitors are similar in price to the bigger streaming services.

SoundCloud uses a fan-powered royalty system where artists' earnings reflect the number of listens they receive...a nice change from Apple, which makes it difficult for any but the very top artists to make a living. It costs $4.99 per month for a limited catalog and $9.99 per month for the full catalog. I was able to find full albums by every major artist I plugged into their search, and many new and independent creators have tracks there as well.

Resonate bills itself as "the first community-owned music streaming service—a multi-stakeholder platform co-operative, democratically governed by our members: artists, listeners, and workers," and boasts, "No subscription. No ads. No corporation selling your data. No bots telling you what to like."

I did some searches and couldn't find any big-name artists on the platform—but if you're looking for tunes you might not hear otherwise, resonate could be for you. You pay 1/4 of a cent the first time you play a track, then a little more each time you replay it. Once you reach about $1.40, the track is yours to keep.

TIDAL costs about the same as Apple Music, with an ad-free music library of over 110 million tracks. This artist-friendly service supports many types of players and has apps for desktop, iOS, and Android.

Even better, TuneMyMusic will transfer your music collection to TIDAL from Apple Music, Amazon, Spotify, or other services. The free trial will transfer 500 tracks; unlimited transfers cost $5.50 per month or $24 annually.

The bad news is, while TIDAL gets points for its high-fidelity sound and fair artist pay, many users complain about its buggy app.

I am currently testing TIDAL. For a few days it was plagued with skipping on tracks like an old record, but that seems to have resolved itself. It works great streaming on my TV. I gave it a few bands I like and it created a “welcome” playlist that is spot on.

Thumbs up from me so far…I’ll report back if there are issues.

PODCASTS: APPLE PODCASTS → POCKET CASTS OR OVERCAST

Pocket Casts is the strongest competitor to Apple Podcasts with its streamlined, easy-to-use interface, plethora of controls, and ability to run on iOS, Android, and desktop. Some features require an upgrade to Pocket Casts Plus, which costs $3.99 per month or $39.99 per year.

If that sounds like overkill, try Overcast, a simple, privacy-respecting, and feature-rich podcast player for iPhone, iPad, and Apple Watch. Overcast is free, supported by small visual ads to promote podcasts, or costs $14.99 per year for an ad-free version.

WIRELESS EARBUDS: APPLE AIRPODS → SONY WF-1000XM5

Engadget gave these Sony wireless earbuds their highest rating in 2025, saying, “With the WF-1000XM5 flagship earbuds, Sony improves its already formidable mix of great sound, effective ANC and handy features. [...] Sony still manages to pack in more features than anyone else too, including trademark ones like adaptive sound and Speak-to-Chat.”

CHAPTER 24

SAY MMM-BYE TO MICROSOFT

Microsoft has been accused of war profiteering and tax evasion. It blocks apps on Windows 11 that allow users to choose the browser and search experience they want.

The company has literally rejoiced that their dominance makes it hard for consumers to move to, and developers to create products for, a new platform, as per this internal memo:

> [...] It is this switching cost that has given the customers the patience to stick with Windows through all our mistakes, our buggy drivers, our high TCO (total cost of ownership), our lack of a sexy vision at times, and many other difficulties [...] Customers constantly evaluate other desktop platforms, [but] it would be so much work to move over that they hope we just improve Windows rather than force them to move. In short, without this exclusive franchise called the Windows API, we would have been dead a long time ago.

The fact that Microsoft is so cavalier about wasting my precious time on this earth was enough for me to drop them like a hot rock. If you feel the same, here are some ideas.

GO BACKWARD

See Chapter 21: Say Goodbye To Google for privacy-forward replacements for Edge Browser, Outlook email and calendar, Bing search, and other Microsoft products. Then check out these alternatives for software suites and video game consoles.

OFFICE SUITE: MICROSOFT OFFICE → LIBREOFFICE

LibreOffice is a suite of free, open-source software compatible with such formats as Microsoft Word, Excel, PowerPoint, and Publisher. It lets you export your work in many different formats, including PDF. It doesn't offer mobile apps or online collaboration, but I've been using LibreOffice for over a year and have been very happy with it.

If you opt for LibreOffice. make it your default app for opening various types of files. For example, for opening .docx files on a Mac, click on any .docx file and press Command-I to open the information panel on that file. Scroll down and you'll see *Open with*. Click on that and select *LibreOffice*, then click the *Change All* button beneath that. From now on, all .docx files will open in LibreOffice. It works the same way for Excel files, PDF files, and more.

In Windows, right-click on a file and select *open with*. Left-click on *Select other application*, and then click on the LibreOffice icon. Select *Always use selected application to open [type] files*, then press *OK*.

If you're done with Microsoft Office, follow these directions to uninstall it from your computer. Then delete or obfuscate your data in your account online and close the account using these instructions. Keep in mind you will also lose access to Outlook.com, Hotmail, OneDrive, Xbox, Skype, Rewards, and Microsoft Certification.

VIDEO CONFERENCING SYSTEM: SKYPE → SIGNAL

I mentioned Signal earlier; this app offers group calling, group video, and file attachments, and everything is end-to-end encrypted. However, the app does lack some video conferencing features like screen sharing.

VIDEO GAME CONSOLE: XBOX → AN XBOX EMULATOR

Yes, it's possible to play Xbox games without an Xbox (or an Xbox Game Pass subscription).

An emulator is a program that gives you the ability to run software from a different device on your computer. Xemu, for example, is a free and open-source application that lets people to play their original Xbox games on Windows, macOS, and Linux. It supports almost all controllers, up to four at a time.

Emulators may run more slowly than the original device and can suck up a lot of bandwidth…but if you're tired of enabling Microsoft with your time, attention, and dollars, this could be the way to go. Want to give it a try? The Xemu site has a list of compatible Xbox games.

PART 7

LIVE YOUR LIFE

You've read through Disengage, maybe filled out the free PDF worksheets, and perhaps even put some of the ideas into practice. This project will likely never be all wrapped up with a nice bow on top, but we can still make great things happen.

WE CAN ONLY DO WHAT WE CAN DO

This book was based on what I learned as I attempted to disengage myself, as much as was feasible, from the companies that have claimed our lives as theirs to profit from. The 2025 update includes what I've learned from practicing much of the advice in this book for about two years.

I couldn't possibly cover every single tactic you might use to take back your life—to reclaim your data, privacy, attention, permission, content, and dollars from those who would abuse them. Even with all I was able to dig up on how to keep Google from tracking you, for example, I wouldn't be surprised if I covered only 10% of the possibilities.

I also may not have covered the precise privacy-invading, exploitative, extractive, or creativity-killing problem that keeps you up at night. Maybe it's business formats like Spotify, Uber, Doordash, or Netflix. Maybe it's the way you're inundated with solicitations from insurance companies and home warranty businesses the instant you purchase a house. Perhaps you want to be done with Target, Walmart, Tesla, and other companies you believe are harming us.

If there are any businesses you'd like to cut ties with—or troubling privacy practices you'd like to tackle—that I didn't cover here, chances are someone else has already done it, and has written a blog post or a guide to help you.

HOW DO YOU FEEL?

As you work your way through this guide, implementing the changes that make sense to you, do you feel lighter? Are you proud that you were able to keep some of your time, attention, data, and dollars out of the claws of Big Tech? Do you feel less like you're walking around in a constant spotlight?

If so, please help spread the word to our fellow citizens who may be withering under the glare. Remember, this book is free! There is absolutely no catch.

KEEP UP THE GOOD FIGHT

Thank you for reading *Disengage*. I hope this humble book helps you deprive hyper-capitalist companies of at least a bit of your one and only life—and helps keep these companies from buying up our country and our rights.

If you'd like to get in touch, please reach out at PunchingUPpress.com. Visit the site to subscribe to ad-free, no-spam, infrequently sent Punching Up Press emails, where you'll learn about new free books, giveaways, fundraisers that fuel resistance, and more.

For the resources I used in researching and writing this book, visit the *Disengage* Resources Page.

ACKNOWLEDGMENTS

I'd like to thank all the readers of this and the previous edition of *Disengage*...my kind beta readers Leanna and @mstrlaw...and my friends, family, and neighborhood group for their help and encouragement.