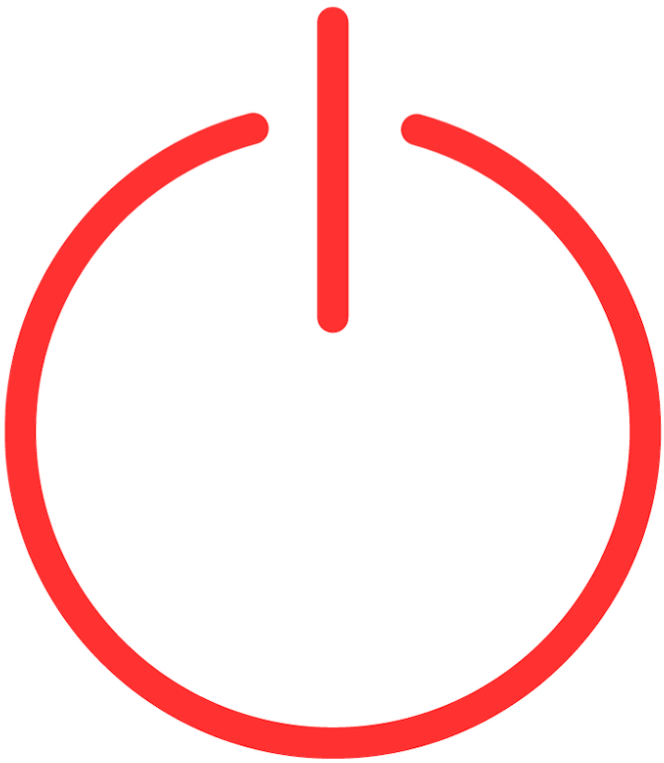
DISENGAGE



Opting Out—and Finding New Options—to Reclaim the Internet from Spammers, Scammers, Intrusive Marketers and Big Tech

By Linda Formichelli

DISENGAGE

Opting Out—and Finding New Options—to Reclaim the Internet from Spammers, Scammers, Intrusive Marketers and Big Tech

By Linda Formichelli

Errata

page 26: OneRep claims to remove your info from 199 sites for $8.33 per month.

[EDITED TO ADD: In April 2024, it was discovered that the CEO of OneRep also founded dozens of people-search firms—meaning he is potentially selling your info on one end, and then charging you to temporarily remove it on the other. I now recommend avoiding this service, especially seeing as how there are others that don’t have a potential conflict of interest.]

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.

For a while 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 goodness knows where. 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, topping taxicabs.

A few times, your wallet is stolen. You 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 Big Tech and the internet, 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 career as a freelance writer in 1997, most of my business was conducted in the library and post office. Over time, however, the internet became my go-to for researching magazine article ideas, finding and contacting expert sources, researching markets, sending pitches and sales letters, and marketing my classes for writers.

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 The Bad Ads 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. (See it here in the Internet Archive!) The website garnered some attention, but I shut it down when I became too overwhelmed with paying work to keep it up.

The spirit of BadAds 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 the Bad Ads Weblog always lived in me:

- I was an active member of SPAM-L, a listserv of mostly software types 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?"

- A friend and I started Renegade Writer Press, which published books for freelancers about how to make a good living by breaking rules.
- I stopped offering mailing list sign-up incentives and chopped our list from 10,000 lurkers to 800 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 gurus, and Google-pleasing content formats in order to stay afloat. (Micro content! No, longform content!)

Outside of business, I was tired of finding my personal information where it shouldn't be, and having my private details compromised in data breach after data breach. I hated that marketing companies were privy to intimate details about my family, income, spending habits, hobbies, voting record, and real estate—which they used to sell me solutions to problems I never knew I had. I resented being forced to buy from megacorps because the products I needed were no longer available anywhere else.

Even more, 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 an unfortunate slip would be caught on someone's doorcam and end up on social media. Yet I experienced the irresistible pull to check in online all day long, 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 structural problems require structural solutions.

I get it. We clearly need to push for better privacy legislation and stronger antitrust 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, middle-aged lady who doesn't like politics, protesting, or public speaking—could do about it.

Not to mention, it took 40+ years to get 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 until all the right societal changes finally kick in?

Here's the great news: We individuals *do* have some 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 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 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 helped me. There are no affiliate links in the guide, and it's free. I don't track who downloads the guide. Please share it!

What You'll Learn in This Guide

Disengage offers my experiences and advice in the following areas.

PART 1: Why Disengage?

Here, I quickly discuss the concepts of surveillance capitalism, chokepoint surveillance, and the exploitation of our common spaces. You'll also discover the side benefits to opting out of Big Tech, and get a reality check on how much of our power we can reasonably reclaim.

PART 2: Disengage By...Reclaiming Your Data

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

PART 3: Disengage By...Reclaiming Your Home

You'll keep strangers from peeking into your home by hiding your home address, removing interior and exterior photos of your home from real estate sites and street view apps, and keeping smart home products from tracking and sharing your (very) private data.

PART 4: Disengage By...Reclaiming Your Content

Did you know that your unpaid content is the very backbone of Big Tech? 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 keep your data secure 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 internet and the hypercapitalist companies that have taken it over. This section will share advice on how to annihilate ads (pop ups, video ads, and the rest), as well as ideas for ditching the most distracting gadget ever created: your smartphone.

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

Hopefully, the previous sections 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

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.

FURTHER READING

These are the books and websites I read as I researched this book. Since I could barely scratch the surface in this short guide, I hope you'll delve into these amazing resources.

Note that this PDF version (as opposed to the online text) includes worksheets at the end of each section to help you get clear on your personal goals, make plans, and gather resources.

The Requisite Caveats

This guide isn't meant to be the final word in disengaging. If you feel you're in danger of any kind—for example, you're being stalked, in an abusive relationship, or being doxed—you'll likely need stronger methods than the ones I outline here. While these guidelines can help increase your privacy, they're mainly meant to improve your lifestyle and to fight back against surveillance capitalism (which we'll talk about later in this guide).

While I did my best to cover as much ground as I could, 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 and offer instructions on how to revoke access for every single case.

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 I'm 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've even created 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. 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 tech-heavy 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, but I won't go into too much detail. 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 the available cash for products and services—within reason, of course—that take care of

some of the related tasks for me. I also have no disabilities or medical situations requiring online solutions, and don't belong to a marginalized group that can find support only in online communities.

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

- All of the products I recommend are free or have free alternatives.
- You decide how much time you want to put into this project.
- You get to pick and choose whatever 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 or resources 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.

Even better, most of the effort required is front-loaded. Once you get your chosen systems set up, they should run as smoothly for you as you 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.

PART 1
WHY DISENGAGE?

The biggest threats we're fighting against in this guide are surveillance capitalism, chokepoint capitalism, and the exploitation of our common spaces; 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 internet companies, including Google, Facebook, and Amazon. While I will give a brief overview of the ills created by each one, I won't get into lengthy critiques of them in this book, 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*[1], 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.[2]

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, where the companies know everything about us, yet we're not privy to how they track, 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 on 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 too high because your entire library of books is now on your Kindle.

This is a very, 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

[1] www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694
[2] news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy

highly recommend reading *Chokepoint Capitalism* by Rebecca Giblin and Cory Doctorow[3], as well as subscribing to Doctorow's ad-free, non-tracking newsletter.

The Exploitation of Our Common Spaces in Under 200 Words

The hypercapitalist businesses we're railing against 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, have our conversations on the platform, and share our news there—giving Facebook more and more of our most intimate data.

Surveillance capitalism, chokepoint capitalism, the exploitation and mining of our personal spaces and relationships: We are nurturing the businesses to blame for these societal ills by constantly feeding them with everything they need to thrive.

[3] www.penguinrandomhouse.com/books/710957/chokepoint-capitalism-by-rebecca-giblin-and-cory-doctorow

CHAPTER 2: HOW DO WE RECLAIM THE INTERNET BY FLEEING IT?

How can I call it taking back the internet when I'm recommending we disengage from it?

It's because *we are the freaking internet*.

When we leave, we take everything with us: our data, our content, our attention, our money. Without all this, the exploitative businesses that have taken over the internet can't survive. In other words, when bigger players are pushing you around the court, you take your ball and leave. When you go off and play with nicer people, the bullies are left with nothing.

The Side Benefits to Disengaging

Maybe it's wishful thinking to believe we can do enough damage to make these megacorporations change their invasive and exploitative practices. But even if we lose this battle, we can still win the war by claiming 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.[4]

So it makes sense that the less data of yours is available, the less likely criminals will be able to use it against you.

[4] onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59

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. 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 little vibration when we 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 as it's meant to be.) We see photos of a well-groomed mom with a perfectly dressed and clean baby and wonder what's wrong with us that our lives don't look like that. We see images of an incredible family vacation and feel like a failure because our toddler cries at Disney. We watch a video by a fitness influencer who tells us he looks the way he does because he lives on 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 sponsors of that vacation.
- That the fitness influencer straight-up lies about his eating habits because he's sponsored by a protein shake company...and also that he works out six hours per day and takes steroids.

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.[5]

Of course, those of us who are in careers, businesses, or school often aren't in a position to simply drop off the internet. 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 the internet, no matter what I did, I would unconsciously start to put together a social media post about it in my mind. How can I make this thought sound more insightful? What hashtags should I use? How should I phrase the post? How should I frame the photo?

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 put it up on my own website and trust 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. When I was on Instagram, Reddit, and various online forums, my first instinct when I couldn't figure something out was to head to one of these sites to ask other members for their input. Do the

[5] www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work

colors in this painting 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.

And 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. When I wrote an article for a client about voice search, my expert source mentioned that businesses were noticing that many searches started with "Should I…?" My source rejoiced over people turning to faceless corporations to help make life-altering decisions—and offered up ways to take advantage of this fact by providing answers promoting a product or service.

When I started to disengage, I had to rely 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 paint in whatever colors are pleasing to my eye because I'm hanging the paintings 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.

Now if I have a question or problem, I research it on my own, take my own preferences into account, and make my own decision. Did you know you can do that? I didn't, because the internet makes it so easy to ask for advice and validation, my decision-making muscles had withered into nothingness.

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

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

Did you know you're a content producer? Everything you post online is used by social media companies, retailers, publishers, travel agencies, supplement sellers, and other businesses to gain legitimacy, engagement, and, ultimately, more eyeballs on whatever it is they're trying to sell. Not to mention, they use that content to gather data from you and from everyone who engages with it.

When you post an inflammatory remark on Twitter—sorry, I just can't call it X—the firestorm of outrage benefits the platform and its advertisers, while impoverishing you and your followers. 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 you don't even get paid for it! 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 and selling our 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 by:

- Learning to think about a purchase before running to Amazon the instant you decide you need something.
- Freeing yourself of your Amazon Prime subscription, encouraging you to look for lower prices elsewhere. (As you'll learn later in this guide, Amazon actually does *not* prioritize good deals.)
- Purchasing cheaper alternatives to overpriced smartphones.
- Seeing fewer ads enticing you to shop, shop, shop.
- Earning more in your business because you aren't spending your time on ineffective social media marketing.
- Buying fewer apps (which also saves you a bundle on in-app purchases).
- Turning to free, open source software in place of some of your subscription-based software.

Who knew disengaging could put more dollars into your pocket?

Side Benefit #9: We inspire others...and ourselves

When you make choices different from what most others are doing, it stands out. And people want to know about it! For example, many people have asked me about my weird-looking non-smart phone. Even my optometrist asked about it.

This gives 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 about these things.

On top of that, each 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 the internet and never look back. Consider this guide an idea book; it's a list of strategies you can pick and choose from depending on your wants, needs, resources, and abilities.

However, we do need to consider the forces working against our desire to disengage:

Force #1: The Enemy Is Overpowered

Thousands and thousands of smart people are working 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, or generally living our lives to fight back with the same intensity.

First of all, 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," according to PCMag. "Even if you deleted all your accounts and never used them again, they'd still probably be able to harvest data on you."[6] For example, Amazon Web Services hosts 6% of the sites on the web—50 million live sites, more than any other web hosting service. (Google is in second place.[7]) Chances are, you will be on an Amazon-hosted site today.

Second, 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.

These 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 clause from the privacy policy of a school yearbook company, of all things:

> 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.

[6] www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one
[7] kinsta.com/aws-market-share/

Dare so much as to buy a yearbook and they've got you. So, yeah…we're fighting against giants in the dark.

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, gather home repair quotes, 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 clear all your data off the internet…and then your kid joins a sports team. The team might require parents to communicate via an app, upload medical forms to a portal, and use yet another platform to volunteer at the concession stand. Suddenly, three more businesses have your info, not to mention all the third-parties they share your info with.

Or maybe you get a job that requires everyone to have accounts on Slack and Zoom. And they publish personal details in your staff bio online. And you have to sign up for a special system to receive your paycheck via ACH. And your boss expects you to extol the company on LinkedIn. Boom! Your data is now in four more places online.

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 can, 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.

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. If you're a member of the school board, a bakery owner, or a stand-up comedian, some 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 authoring books, selling courses, and writing for magazines both print and online. I marketed on social media, did interviews with the press, joined business and writing groups online, was a guest on podcasts, and 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 still reap benefits from anything we manage to accomplish toward this goal.

NOTES ON PART 1

Why do I want to disengage?

What information about myself or my family do I consider off-limits for corporate surveillance?

Where do I experience surveillance capitalism online or in my life?

Where have I noticed chokepoint capitalism? Where is there a useless business getting between me and a product or service I want to download, use, or purchase?

How has corporate surveillance affected my relationships or the public spaces I use?

PART 2

DISENGAGE BY... **RECLAIMING YOUR DATA**

Our data is the most nourishing possible sustenance for Big Tech. 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 an acquaintance who vigilantly protected their data from the first moment they went online over a decade ago. Their real name appears in only two places on the entire internet, and those instances are obscured by the hundreds of other people who share this person'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: START READING 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."[8]

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 are 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?

Despite all 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.

8 pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

CHAPTER 5: CONTROL YOUR ONLINE ACCOUNTS

This part can be fairly time consuming, but it's also easy to do in chunks during spare moments of time. Waiting for a Zoom meeting to start? Sitting in a waiting room? Bored between events at your kid's track meet? 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.

I made you a spreadsheet

Download my Excel template for free, which you use on your desktop computer or upload to Google Sheets, Zoho, or another cloud-based spreadsheet platform. You'll find separate tabbed sheets for accounts, people-search sites and data brokers, bios, and reviews—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 about.

Be sure to also check your bank and credit card transactions to dig up businesses that have your info; for example, you may remember 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 your 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, 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, you can 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 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? You may find 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.) Those accounts are an easy place to begin.

Step 1: Request Data Deletion

Before deleting 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 delete 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 retain your information in their database.

Step 2: If That Doesn't Work, Obfuscate 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 you can do in this situation.

Step 3: Delete the Account

Once your data is deleted (or obscured), 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 by people who have figured it out. Some people have also compiled lists of how to delete notoriously difficult accounts.

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 really don’t 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.

My 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, maybe this tactic will throw a little chaos into surveillance capitalists’ databases.

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.[9]

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

The good news is, you can opt out of most of these lists. The bad news is, 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.

A friend of mine made a project of opting out of a handful of them 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.

If you're low on time and have some cash to throw at the problem, services like DeleteMe (the one I use) will handle this for you on a quarterly basis and send you reports with the results. It 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).

[9] epic.org/issues/consumer-privacy/data-brokers/

These are some similar services:

- OneRep claims to remove your info from 199 sites for $8.33 per month. They offer a free scan; I tried it, and the service found my info on only six sites since I had already been using DeleteMe for a while. You could use this scan as a starting point if you want to opt out of people-finder sites manually. [Not recommended — see erratum]
- 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 pretty pricey.
- EasyOptOuts is only $19.99 per year and claims to opt you out of over 160 sites.
- Privacy Pros offers a premium service for $999 per year that asks Google to remove links to your profile as they're taken down from people-search sites. (You can do this on your own! 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 services, many of them offer free guides and other resources for DIYers.

These services don't catch every single people-finder site—there are *a lot* of them, and some don't allow third parties to opt people out—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.

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 cases, I used a masked credit card to pay for a monthly subscription, then canceled right away. (Even if the site continued to charge me, fraudulently, I only loaded the card with enough money for one month).

Bash the Brokers By...Focusing on the Biggest Villains

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 broker, the bigger the data breach. In 2017, an Equifax breach compromised the personal information of more than half the people in the U.S., and 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 super 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 to criminals.

Some of the paid consumer privacy protection sites 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 go back and choose a different option, such as asking them to not share your info.

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

How to opt out of Acxiom

From the Acxiom opt-out page: "Acxiom provides consumers on a nationwide basis with various rights with respect to their personal information, including a right to know the information that Acxiom has them, the right to request the deletion of their personal information , and the right to opt out from the sale of their personal information."

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

How to opt out of Epsilon

Epsilon lets you request they not share your data, make a deletion request, and more; however, you're allowed to select only one of the eight options at a time through the website, meaning you may have to go through the (quick) process multiple times depending on your needs.

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

Oracle will let you opt out of cookies from Oracle Advertising and will delete all data associated with these cookies. In addition, according to their opt-out page, you can "opt out of the use and sharing of your personal data for offline direct mail campaigns and for online interest-based advertising facilitated by Oracle Advertising."

Opt out of Oracle by filling out this form.

How to opt out of LexisNexis

LexisNexis boasts *billions* of records, including data from 1.5 billion bankruptcy records. The company allows you to opt yourself and family members living at your address out of their data products, but warns you may experience "future difficulty using online systems for such things as instant identity and insurance verification." However, after I made my request, I received an email with a link to use if this happens.

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 to its marketing customers that "goes beyond age and gender." The company advertises data such as purchase history from more than 90 million households, and even a personality survey on individuals, according to the Sanford School of Public Policy at Duke University.[10]

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. You may want to enter every email address you have just to be sure *all* your data is deleted.

How to opt out of CoreLogic

I had to wade through a lengthy privacy policy to figure out how to opt out and request data deletion from CoreLogic! The answer: Send an email to privacy@corelogic.com. If you're in the EU, email privacy@corelogicsolutions.co.uk. They don't provide any info on *what* to email them, so be sure to include your name, email, and address, and request they cease sharing your information with third parties and delete your data. (It sounds like they may not comply with deletion if you aren't in a protected state, but it doesn't hurt to ask.)

The credit agencies Experian, Equifax, Innovis, and TransUnion are other massive companies brokering your data, but they are a special case. We'll discuss how to opt out of them in the next section.

---

[10] techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf

How to opt out of Foursquare

This one is a little bit of an outlier, but I thought it was worth mentioning. 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.

As for Apple users: As of iOS 14, you have no way to access your IDFA without using a third-party app such as the low-rated Find My IDFA or the unrated Get My IDFA. 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.

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

Making sure your IDFA is set to private on your Apple devices should keep them out without you having to dig for your ID. Go to Settings, navigate to Privacy, select Advertising, and set your IDFA to private.

Bash the Brokers By...Leaving the Lists

Businesses use the data collected by brokers to compile lists of people they then target with ads, credit offers, and more via email, mail, and phone. Here's how to get your name removed from these lists.

This goes a bit beyond the theme of disengaging from the internet, but remember that much of what you do offline ends up online, and vice versa. For example, according to an article in The Markup, your local grocery store not only collects data on your purchases, it even tracks you as you wander around the store.[11] They certainly don't keep all this info in physical file cabinets or on non-networked computers!

That's why, in this guide, I attempt to tackle the problem on as many fronts as possible.

[11] themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

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'd like to counter with this: If it gets immediately thrown into the recycling bin, that's *the definition of junk*. Here's how to stop it 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 $4 to remove up to five household members' info for 10 years.

Return to sender

Certain businesses and groups—such as companies you've done business with in the past and charities—aren't required to remove you from their lists. But guess what? 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.[12] If the sender is smart, they'll remove you from their mailing list. This process will probably be very slow, but over time it should make an impact.

Another easy (but also slow) option is to write "Remove me from your mailing list" on the offer, stick it in the pre-paid reply envelope you'll find in many 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 the worst direct-mail offenders; the directory provides instructions on how to remove yourself from various businesses' lists. The directory is not at all comprehensive, but does include major mailers like AARP and MasterCard.

How to remove your name from prescreened credit offer lists

Those companies that generate your credit score—Experian, TransUnion, Innovis, and Equifax—do more than influence whether you get credit (and how much). They also sell your data to businesses so they can 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."

[12] faq.usps.com/s/article/Refuse-unwanted-mail-and-remove-name-from-mailing-lists

You can 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 from ValPak mailings 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, you can 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 its lists.

This won't stop spam, as actual spammers notoriously don't clean their lists of people who don't want to receive their crap. But again, 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 don't care whether or not you want their calls.

CHAPTER 7: SURF IN SECRET

Disengaging from the internet completely is a pipe dream for most of us. If you don't want to (or can't) 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.

Surf in Secret Idea #1: Rewrite Your Life Story

You created a nice little 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, if you're like me, you feel you can't disengage from the internet when so much information about you is so easily accessible online. 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 change or erase your information.

It's not always easy. For example, changing my author bio on Goodreads was a pain. And editing it on Google was literally impossible! After many attempts to claim my "Knowledge Page," I finally gave up when Google switched my bio to one I used years ago (and also 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 websites 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 freelance writer, I spilled details about my life in bios and interviews everywhere from print magazines to my Amazon Author page. I contacted magazines and book publishers I wrote 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 writer—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 an interview an old client did with me to offer advice to their freelancers. The interview was fairly up to date, it shared valuable information, and it wasn't overly personal. While I would rather have the interview 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 who I asked complied with my requests. One podcaster told me he couldn't remove the actual interview with me because it would create a hole in the catalog—but he did remove the website page it was hosted on as well as the podcast notes, making it more difficult for the casual web surfer to find. I was thankful for the compromise.)

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

So you've gotten your bios removed from some sites and edited on others. 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. You can speed this up by using this link to ask Google to remove or reindex outdated content. 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 not show up in DuckDuckGo.)

Surf in Secret Idea #2: Control Your (Actual) Image

If you're a typical internet user, your photo is everywhere. Your company's "About Our Staff" page. Facebook. Google's image search. And so much more.

Some of this you may not want to (or be able to) change or delete. Your company might not be cool with you having a blank square as your professional headshot, and you can't go in and remove your photos from all your friends' Instagram posts. For safety reasons, a Meetup group 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?)

Step 1: Get creative

Have some fun with it if you can! I changed my Amazon headshot to a photo of me taken during an acting job, where I look nothing like my real self. On other sites, I swapped out my photo for images of my oil paintings. Any staff member at my doctor's office who looks at the portal profile I mentioned above is treated to a painting instead of my real mug.

Step 2: 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 an oversight, such as an old employer who forgot to remove you from their massive "About Our Employees" page.

Step 3: 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 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.[13]

Here's where you can 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. (This includes all kinds of content, not just images.)

Surf in Secret Idea #3: Use 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.

[13] support.google.com/websearch/answer/6302812?hl=en

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 wi-fi hotspots safely, meaning you can use the free wi-fi at say, Starbucks without worrying about your activity being intercepted by a bad guy.

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

I use the VPN bundled with my Proton Mail subscription (see Chapter 20: Say Goodbye To Google for more info on Proton), which was rated as Best Overall VPN by PCMag.[14] Others in the top 10 include:

- NordVPN
- Surfshark
- TunnelBear (Rated Best for First-Time VPN Users)
- ExpressVPN

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.

Beware: Free VPNs also 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 your 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 Idea #4: Throw 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.)

[14] www.pcmag.com/picks/the-best-vpn-services

Here's how to keep cookies from tracking you and sharing your data. Before you follow any of these instructions, please 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. Generally, you can 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 offer this easy option, 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

You can also 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 in to every service you use each time you use it (assuming you've logged out), 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 Chrome

1. Click on the three-dot menu in the upper right of your Chrome browser.
2. Go to *Settings.*
3. Go to *Privacy and security.*
4. Click *Cookies and other site data.*
5. Click *Block third-party cookies.*

How to disable cookies in Firefox

1. Click on the three-line menu on the upper right.
2. Click *Settings.*
3. Select *Privacy & Security.*
4. Choose *Standard*, *Strict*, or *Custom*. Note that the Strict setting may affect how well some websites work. The Custom setting lets you adjust how trackers are blocked.
5. Use the directions above to go back to *Privacy & Security.*
6. Set *Do Not Track* to *Always*.

How to disable cookies in Safari

1. Go to *Preferences*, then *Privacy.*
2. If the box for *Prevent cross-site tracking* doesn't show a check mark, click to enable it.
3. Go to *Manage Website Data*.
4. Click *Remove* next to the trackers you want to trash, or *Remove All* at the bottom of the screen to dump them all at once.
5. Finally, check the box for *Block all cookies.*

How to disable cookies in Microsoft Edge

1. Click on the three-dot menu in the upper right corner.
2. Choose *Settings.*
3. Select *Privacy and services* from the menu on the left.
4. Choose the *Basic*, *Balanced*, or *Strict* privacy setting. Note that the Strict setting may affect how well some websites work.
5. Follow the steps above to go back to *Privacy, search, and services.*
6. Disable *Help improve Microsoft products by sending optional diagnostic data about how you use the browser, websites you visit, and crash reports.*

When you disable cookies in your browser, future attempts to place cookies on your computer will be blocked. But what about all the cookies already chilling on your computer? You'll need to trash them; see more below.

Option 4: Let browser extensions do the work

An extension—sometimes also called an add-on—is software that adds features to your browser; for example, you may be familiar with the Honey x PayPal extension, which searches for promo codes when you're about to pay for your order in an online store. 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. When I was using the Chrome browser I opted for Privacy Badger, which was created by the nonprofit digital rights organization Electronic Frontier Foundation. It was easy to install and worked great. To find a free cookie-crumbling extension for your browser, check out Chapter 18: Annihilate Ads.

Defeat the super cookie

Even more troubling than third-party cookies are super-cookies: cookies placed on your computer by your Internet Service Provider (ISP), the company that provides your internet connection. The ISP sells the data to third parties, and you can't block these cookies. Worse, your ISP can restore deleted cookies. You just can't get rid of them!

The only way to prevent your ISP from putting super cookies on your computer is to use a VPN. See the next chapter for more details.

Final Step: Empty the cookie jar

So you chose one of the options 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. Keep in mind that once you clear cookies, you may be logged out of any websites you're signed in to.

How to clear the cookies in Chrome

1. Click the three-dot menu on the upper right.
2. Select *History*.
3. Choose *Clear Browsing Data*.
4. Set the Time Range to *All Time*.
5. Click to check *Cookies and other site data*.
6. Select *Clear Data*.

How to clear the cookies in Firefox

1. Click on the three-bar menu on the upper right.
2. Click *History*.
3. Choose *Clear Recent History*.
4. In the popup, set the time range to *Everything*.
5. Check the boxes to clear *Cookies* and *Offline website data*.
6. Click *OK*.

How to clear the cookies in Microsoft Edge

1. Click the three-bar menu on the upper right.
2. Open the Settings menu.
3. Select *Privacy, search, and services*.
4. Under "Clear browsing data," select *Choose what to clear*.
5. Select *Cookies and other site data*.
6. Click *Clear Now*.

How to clear the cookies in Safari for Mac

1. Click on *Safari* in the menu bar at the top of the screen.
2. Select *Settings*.
3. Click the Privacy tab.
4. Click *Manage Website Data…*
5. Select *Remove All*.
6. Click *Remove Now*.

Again, these instructions are for the browsers on your desktop computer and not your devices; the steps for doing this in your browser app may be different. In all cases, you may need to quit and restart the browser for the changes to take effect.

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.[15] That's more than one full workday out of a 9-5 workweek! Not only is email distracting and time-consuming, everyone from spammers to small shops to big businesses use it to track, target, and harass us.

In Chapter 20: Say Goodbye To Google, we'll talk about ditching your email provider for a more privacy-forward one. But if you want to stay put, 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...Using the "+" Trick

You can 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 enter your email in the pop-up for a Nike discount as xyzabc+nike@gmail.com. Emails to this address will still reach you.

If you start getting unwanted mail addressed to a subaddress, you can quickly set up a filter to automatically delete any emails sent to that address; this is easier than trying to set up separate filters on every sender who mails you there.

This trick also allows you to use one email address for different purposes, instead of maintaining multiple addresses to protect your main email. Unfortunately, however, it's trivially easy for marketers to clean their mailing list to remove the portion after the "+" symbol.

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.

[15] www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work

This is not rare: When I ran a business of my own, every email marketing provider, from Mailchimp to AgileCRM, offered tracking. It 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. I used to use a tracker extension to keep an eye on my magazine pitches; when an editor opened my pitch, I would make a note to follow up a couple weeks later. Not to mention, some people, even if they're not emailing you for commercial purposes, just like to track whether and when their emails are read.

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 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.[16]

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 options exist. Most extensions will walk you through set-up.

[16] mikeindustries.com/blog/archive/2019/07/superhuman-is-spying-on-you

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 cheap to create additional email addresses. Then you can decide who gets which address.

I pretty much abandoned the Gmail address I've had for years, which has appeared in just about every data breach, data broker database, and people-finder site out there. (I actually stopped using Google products as much as I possibly can; see Chapter 20: Say Goodbye To Google for how you can do the same.)

In the meantime, I created a private email address on my domain I shared with only my family members and closest friends. I then created a second address to give to people and businesses I trust, but who aren't in the inner circle. People and businesses I have no reason to trust get a masked email; more on that below.

Escape Email Tracking By...Masking Your Email Address

A masked (or anonymous) email address hides your information while forwarding emails to the real address of your choice. If 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, you can quickly delete an anonymous address if you start getting spam there—which you can't do so easily with your real email address.

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

- DeleteMe, the company I hired 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?
- Proton, 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.

If you, like me, want to be pretty hardcore about it, you can create a separate masked address for every purpose. For example, I have different addresses for my grocery store, my credit card company, my bank, etc. Both Proton and DeleteMe let you turn off addresses as needed, and there doesn't seem to be a limit on how many you can make.

Two caveats

First, this tactic can make a mess of your passwords. Unless you have a password manager like LastPass or 1Password, you'll need some way to store or remember which address you used on what accounts when you sign in. (FYI, Proton offers a free password manager.)

Second, if you think 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—and the more businesses you gave a masked address to, the more you'll need to go in and change. In this case, it's safer to use masked addresses only for companies you're pretty sure you won't be doing business with in the future, and to use one of your real addresses for your credit card, utilities, and so on.

The idea of this is not just to protect my personal information, but also to confound Big Tech. I love the idea of a broker having an entry for me with 50 email addresses (and a couple of aliases, and a PO Box in addition to my home address, etc.). 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, right?

Escape Email Tracking By...Using a Privacy-Forward Email Provider

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

- 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 $12.99/month for more features, 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." The free email includes a calendar and 1 GB of storage. Upgrading (€3/month—that's $3.21 as of November 2023) 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 50 MB of storage for emails and 50 MB for documents. Upgrading ($3.50/month) will get you more storage, the ability to use a custom domain, and more.
- Posteo offers “a secure, ad-free email account powered by 100% green energy” for just €1 ($1.07 as of November 2023) per month.

Many of the secure email providers are based in EU countries, which have stronger privacy protections—hence the prices in Euros. 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.

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. (Not to mention all the spam texts and telemarketing calls they deliver to us!) And yet, they've become a necessity. Below, you'll learn how to protect your data and your privacy when using your phone.

Protect Your Phone • Idea #1: Get a Secondary Number

Free throwaway phone numbers are easy to get, but I've found most businesses have wised up, and their online forms will now detect and reject these numbers. A better bet may be to mask your phone number using a paid service like DeleteMe; this lets you generate numbers that will ring on your real line. You could also create a secondary number using Twilio to use in online forms, for loyalty programs, and so on.

Of course, there's also Google Voice, but if you go this route you're just supplying even more information to Google. The choice is yours.

Protect Your Phone • Idea #2: Use 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 premium versions, also play an "out of service" recording, which encourages the caller to remove you from their list.

Protect Your Phone • Idea #3: Hide Your Location

Investigative reports have shown that your phone's location data may be for sale.[17] If you'd rather not have details on your whereabouts gathered and sold for commercial purposes, it's important to control your phone's location tracking.

[17] www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood

How to disable location tracking on iOS

There are three levels of protection on iOS: You can disable Significant Locations, which records your frequently visited locations; disable location tracking for selected apps; or turn off location tracking altogether.

Option 1: Disable Significant Locations on iOS

1. Open the Settings app.
2. Tap *Privacy*.
3. Tap *Location Services*.
4. Tap *System Services*.
5. Select *Significant Locations*.
6. Tap the toggle next to “Significant Locations” to OFF.

You can erase the data Significant Locations has already stored by clicking Clear History on the Significant Locations menu.

Option 2: Disable location tracking for specific apps on iOS

1. Open the Settings app.
2. Select *Privacy & Security*.
3. Select *Location Services*.
4. Make sure "Location Services is on.
5. You’ll see a list of your apps. Tap on an app and select whether and when you want it to be able to access your location information. For many apps, you can safely click *Never*. If the app needs to know your location to work, such as a maps app or Find My iPhone, you can require it to ask you before accessing your location; another option is to let it use your location only when you’re actually using the app.

Option 3: Disable location tracking altogether on iOS

1. Open the Settings app.
2. Select *Privacy & Security*.
3. Select *Location Services*.
4. Toggle “Location Services” to OFF.
5. Tap *Turn Off* on the warning banner.

If you’re afraid to turn off location tracking altogether, keep in mind you can always turn it back on if it starts affecting features and apps you need.

How to disable location tracking on Android

You can disable tracking altogether for various features, as well as select which apps you would like to have access to your location data.

Option 1: Disable location tracking for specific apps on Android

- Swipe down from the top of the screen.
- Long-press the Location icon in the Quick Settings menu.
- Tap *App permission* or *App location permissions* (for Android 12).
- You'll see a list of your apps. Click to allow the app to use location data all the time, only while in use, or never, or to require the app to ask you before accessing your location. You can also decide whether an app is allowed to use your "precise location," which uses other types of tracking in addition to GPS; if you allow it, Google Location Accuracy on the Location page will also need to be turned on.

Option 2: Disable location tracking altogether on Android

- Swipe down from the top of the screen.
- Long-press the Location icon in the Quick Settings menu.
- Toggle Use location to OFF.
- Tap *Advanced* or *Location services* (for Android 12).
- From here, you can toggle on or off location services for various features, such as:
    - Google Emergency Location Service, which you probably want to keep turned on.
    - Wi-fi Scanning, which lets the device scan for wi-fi even when wi-fi is turned off.
    - Bluetooth Scanning, which lets the device scan for Bluetooth even when Bluetooth is turned off. Wi-fi and Bluetooth scanning are both used to improve location features. If you don't see them on the list of features you can toggle on or off, look for a link for "Wi-fi and Bluetooth scanning" on the Location page.

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 • Idea #4: Be 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.[18]

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 options for safely using many apps are to give them fake 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 whatever data sharing you can.

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.

[18] surfshark.com/apps-that-track-you

CHAPTER 10: STOP BEING LOYAL

You're about to buy a mattress-in-a-box online, and a pop-up appears offering you a discount in exchange for your name and email address. You enter the info, and another 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. Not only that, for every $100 you spend, you get a $5 coupon.

I used to write for 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 businesses also sell your information, opening up yet more opportunities for the data to be stolen by criminals.

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.'"[19] One billion dollars! Can you imagine any grocery store passing up that kind of money?

So if you're fortunate enough that you can choose not to 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 seems like a sweet deal, the good news is that once you've put some of the privacy practices from this guide into place, you can use these tactics to 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, but at least the mass of fake data might help hide the real stuff.

[19] themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

NOTES ON PART 2

Which steps will I take to keep my personal data from falling into the hands of surveillance capitalists?

- [ ] Download the free spreadsheet and work on my accounts: delete ones I don't use, request data deletion, edit my personal information, or update my privacy preferences.
- [ ] Hire a company like DeleteMe to remove my info from people-search sites, or go through the list in the spreadsheet manually to opt out of these sites.
- [ ] Use a cookie-blocking extension or reject all cookies in my browser.
- [ ] Clear cookies from my computer.
- [ ] Get a secondary phone number.
- [ ] Disable location services on my phone or on certain phone apps.
- [ ] Get a secondary email address.
- [ ] Use a service to create masked emails.
- [ ] Delete these loyalty accounts:

- [ ] Delete/replace/update the privacy settings on these apps:

- [ ] Other:

What obstacles are keeping me from accomplishing the tasks I want to do?

How can I overcome these obstacles?

What resources do I need in order to accomplish these tasks, and where can I get them?

I plan to have these tasks completed by DATE:

PART 3

DISENGAGE BY... **RECLAIMING YOUR HOME**

The businesses claiming the internet as their profit-boosting playground don'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 business collects your mail and sends you photos via email or in their app. You can ask the company to trash mail pieces for free, or pay a small fee to pick up your mail, request a scanned PDF of the contents, or have the company shred your mail. The company I use, 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—which you can later do with your new PO box address, as well). (See Chapter 6 for more on mailing lists as well.)
- Signed up for paperless billing, statements, etc. where you can.

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

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

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 sites. Many states keep open records on home sales, for example, and if you started a business using your home address, this information often can't be changed in your state's business records online. Even worse, people-search sites get a lot of their info from public records, making it more difficult for you to wrest control of your home address and other data from these companies.

If you have a court order because you've been stalked or are otherwise in danger, you can send it with your request for deletion from public records. But if you just 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 to politely ask how you can 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 say, "See how Maya's neighbors on Gardenia Grove Drive voted!" Real helpful.

There is a bright side: Now that you know all this, you can take pains to use your PO box or otherwise conceal your home address in future dealings.

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 house 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 anyone 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, thank goodness.)

Step 1: Claim Your Home to Delete Interior Images

These real estate listing sites will let you "claim" your home, at which point you can remove the listing photos. Scary fact: Anyone who knows your name and home address 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.

How to claim your house on Zillow

1. Enter your home address here.
2. Click on *View This Home*.
3. Create an account or log in.
4. Click on *Claim Home*.
5. To verify, Zillow will display a list of names; choose your name from the list.

How to claim your house on Redfin

1. Go to Redfin and enter your address.
2. Click on *I Own [Address]*.
3. Log in or create an account.
4. Follow the steps to prove your ownership.

How to claim your house on Realtor.com

1. Go to My Home.
2. Search for your street address
3. Click *Yes, Claim It* in the popup box.
4. Log in or create an account.
5. Follow the steps to prove your ownership.

The fact that it's so easy to claim ownership of someone else's home is also a 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, you ask Google Street View and Apple' Maps Street View to blur your home's image. This is irreversible, though, so make sure it's what you really want to do!

They say you can only blur images of a building you own, not a rented or leased home—though when I went through the Google Maps process it didn't ask for proof of ownership.

How to ask Google to blur the image of your home

1. Open Google Maps.
2. Find and open the 360 photo you would like blurred.
3. Click the three-dot menu and select *Report a problem*.
4. Complete the form.
5. Click *Submit*.

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 smart homes.

What this means *for you* is you can check in on your dog, turn on your lights, or lock the doors no matter where you are.

What this means *for the companies 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 flowing from your home; for example, 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 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.[20]

Worse, many of these products provide little security; when researching this chapter, I found a Reddit thread by someone whose home assistant 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 writes. "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."[21]

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

[20] www.theatlantic.com/technology/archive/2023/09/managing-digital-privacy-personal-information-online/675184/
[21] www.reddit.com/r/homeassistant/comments/ywubxi/bluetooth_toothbrush_privacy_concern/

technologies are tracking you even in your home, you can see 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
- Dishwasher
- Doorbell
- Security camera
- Speakers
- Coffee maker
- Thermostat
- Toothbrush
- Oral thermometer
- Gaming console
- Washer
- Wi-fi-enabled headphones/earbuds
- Dryer
- Vacuum
- Tablet
- E-reader
- Fitness tracker
- Digital camera
- Digital personal assistant
- Exercise bike, treadmill, etc.
- Smoke detector/CO2 detector

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 super 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 to replace it with an old-school one.

Step 2: Update the Privacy Settings for Each Product You Keep

Check out the privacy settings in any apps associated with your smart products, and change them to the highest protection level. You may also need to go into the settings on your smartphone to ensure the products aren't accessing features they don't need—for example, your camera, microphone, location data, or contacts list.

Step 3: Delete Conversations in Products You Talk To

According to PCMag, there have been reports of Amazon employees actively listening to Alexa voice recordings.[22] Google speakers have also been compromised, exposing users' private conversations.[23]

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

Are you pretty skilled with tech? If so, consider a privacy-forward, open-source assistant like Home Assistant, which is "perfect to run on a Raspberry Pi or a local server," though you can also run it on MacOS, Windows, and Linux. The company website has thorough documentation and getting-started guides, but I can see that for many of us, the learning curve would be steep.

If you can't do without a digital assistant in your home, and you don't have the tech know-how to implement a privacy-oriented assistant, at least be sure to delete your conversations on a periodic basis to decrease the chances of your home chatter being compromised by the companies providing these apps—or by criminals.

How to delete your Alexa history in the app

1. In the app, navigate to *Settings*.
2. Go to *Alexa Privacy*.
3. Choose *Review Voice History*.
4. Click the "down" arrow next to *Displaying*.
5. Click the "down" arrow next to *Filter by date*.
6. Select *Custom* and fill in the date range for which you'd like recordings erased.
7. Tap *Delete all recordings from [selected date range]*.
8. Confirm your choice in the pop-up.

[22] www.pcmag.com/news/thousands-of-people-listen-to-alexa-voice-recordings
[23] www.bbc.com/news/technology-48963235

How to delete your Alexa history from Amazon

1. Go to Amazon.com.
2. Hover over *Account & Lists* on the upper right.
3. Choose *Content & Devices* from the drop-down menu.
4. Click the *Privacy Settings* tab at the top.
5. Select *Alexa Privacy*.
6. Click *Review Voice History*. From there, you can delete individual recordings, select a custom date range, or trash all of the recordings at once.

How to delete your Google Assistant history

1. Sign in to your Google Account.
2. Go to your Google Account's Assistant activity page.
3. At the top right, click on the Google Assistant banner.
4. Click the three-dot menu.
5. Select *Delete activity by*.
6. Choose *All time*.
7. Click *Delete*.
8. To confirm, click *Delete* again.

According to Google, when you delete all activity, it may take a day for the activity to be deleted from your other devices.

How to delete your Siri history from Apple HomePod

1. Launch the Home app on your iOS device.
2. Click the HomePod card on the main Home screen.
3. Click the cog icon on the bottom right of the HomePod card.
4. Click *Siri History*.
5. Tap *Delete Siri History*.

How to delete your Siri history from your iOS devices

Starting with iOS 13.2, you can choose whether you want contractors to listen to your Siri interactions in order to improve the service, and also delete existing recordings from Apple's servers.

To opt out of Siri recordings review:

1. Navigate to *Settings*.
2. Go to *Privacy*.
3. Select *Analytics & Improvements*.
4. Toggle *Improve Siri & Dictation* to OFF.

To delete the recordings:

1. Navigate to *Settings*.
2. Go to *Siri and Search*.
3. Select *Siri & Dictation History*.
4. Click *Delete Siri & Dictation History*.

Keep in mind that these assistants also work on your phone, smartwatch, smart TV, car (think Apple CarPlay), smart home products (such as Google Nest), and other devices. If you can talk to a gadget, it probably incorporates a nosy digital assistant. You may need to delete recordings separately from each one; at least in Apple's case, it seems deleting the history on one device only affects conversations dictated through that particular device.

Step 4: 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 bad actors 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, you'll need 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 easy for you as well!

Step 5: Tell Your Car to Stay in Its Lane

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. From there, you can tighten up your privacy choices or ask the manufacturer to delete your data.

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 postal letter, and received a response via mail over two months later.

Step 6: 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.

NOTES ON PART 3

When I get a PO Box, these are the people, businesses, and accounts I'll need to update:

_____ ☐ Updated? _____ ☐ Updated?

_____ ☐ Updated? _____ ☐ Updated?

_____ ☐ Updated? _____ ☐ Updated?

_____ ☐ Updated? _____ ☐ Updated?

_____ ☐ Updated? _____ ☐ Updated?

I need to ask these websites/people/government websites to remove my home address:

_____ ☐ Completed? _____ ☐ Completed?

_____ ☐ Completed? _____ ☐ Completed?

_____ ☐ Completed? _____ ☐ Completed?

Real estate sites to claim my home on/remove interior photos from:

☐ Zillow

☐ Redfin

☐ Realtor.com

☐ Other_____

I need to ask these map apps to blur my home images:

☐ Google Street View

☐ Apple Maps Street View

☐ Other_____

Which of the smart products in my home actually improve my life?

_____

_____

_____

Here's how I plan to keep the smart products in my home from tracking me:

Product: _____ ☐ Replace ☐ Update privacy ☐ Delete conversations

Product: _____ ☐ Replace ☐ Update privacy ☐ Delete conversations

Product: _____ ☐ Replace ☐ Update privacy ☐ Delete conversations

Product: _____ ☐ Replace ☐ Update privacy ☐ Delete conversations

To Do List:

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

PART 4

DISENGAGE BY... **RECLAIMING YOUR CONTENT**

We often say that we are the product of companies like Facebook, LinkedIn, Twitter, 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.[24]

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.

[24] rushkoff.com/books/survival-of-the-richest-escape-fantasies-of-the-tech-billionaires

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 fan fiction discussion 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—I'm saying anything you share online can be scraped by businesses to enrich your profile…and possibly used against you.

Here's what you can do 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?

Option 2: Delete Forum Accounts Altogether

If you want to disengage even more, delete some of your forum accounts altogether. This is another of those instances 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 that the benefits outweigh the disadvantages.

Note that deleting forum accounts may or may not also erase your posts; for example, if you delete your Reddit account, your posts will remain and only your username will be deleted. 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. This method isn't foolproof—there are usually ways people can find deleted posts if they want to, such as by using the Wayback Machine or (for Reddit) platforms like Reveddit.

Again, we can never achieve 100% privacy and anonymity—even if it's what we want to do. My philosophy is to just do as much as I can, and to be more careful in the future based on what I learned going through this 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 whatever did we do before there were so many outlets for us to share our yays and nays? Somehow, we all survived.

When you spend time adding yet another review of the local skate park, you're working for the review site more than your fellow citizens. 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?

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.

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

- Google
- Facebook
- Yelp
- Tripadvisor
- 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 and G2 Crowd
- Employer review sites like Glassdoor

Really, really want to write up a glowing review or to 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 Facebook or Twitter when a book marketing firm ripped me off to the tune of $6,500, 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 well-known science fiction author 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. Things got even better when the culprit was caught using a fake name to post comments on my blog.

Can you imagine a review on, say, 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.

CHAPTER 16: SAY SAYONARA TO SOCIAL MEDIA

What a minefield: We know how bad social media is for our mental health. We know we are the product, and that these platforms mine, use, and sell our data ruthlessly. We know their algorithms serve us negative, frightening, or anger-inducing information—and sometimes just plain lies—because that's what gets engagement. And yet we have such a hard time quitting!

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 forced to use social media in order to sell our art (Instagram!), move our books (TikTok!), or generally promote 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?

That said, there are alternatives. Check out the ideas below to figure out whether it's possible for you to disengage from social media, where to go instead, how to run an online business without these platforms, 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 saying FU to Big Tech, it's worth it to 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. They all want you to look at, click, like, download, and buy their stuff. Your two daily business posts are swept into oblivion within seconds by the sheer number of new posts. Are you really getting any return on your investment of time and energy?

(If you do feel 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, sell things, or just to be entertained, think about what other options are available for meeting these needs.

For example, instead of occasionally selling an item 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, ask local veterinarians to mention you to clients, leave fliers with local businesses, or write pet-related articles for regional publications?

Doubtful? Run a time-limited experiment to see whether an offline option works for you; you may even find you enjoy it more, 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?

In many cases, we feel the need to use social media because we've been trained to think we need everything we do and think to be visible to others, lest we not fully exist. You can probably guess who trained this into us, and how they benefit from our free content.

Until recently, I had an Instagram account to post my art. I'm not 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 tiny, insistent voice 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 art…which I am."

Are you missing out on 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 amazing things and not need to show them off to the world.

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

As I mentioned, I opened an Instagram account after I retired just to post my art. I was more interested in getting other people's approval of my creations than in giving approval myself. And I'm not unique—so chances are, many other people feel 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, I heard from only two people who noticed I was gone. I ended up creating a new LinkedIn profile around 2019 when I started a new business, but never reopened the others.

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 all the rest: When I see them, I wish I could get those seconds of my life back. (And yet it's so hard to stop scrolling!)

Ask yourself when was the last time you actually heard or saw something useful or actionable on social media.

Question 6: Are the people on social media close enough friends for me to deal with the hassle?

I've come to the conclusion that if I learn from Facebook you got married or had a baby, we're not very good friends. Real friends would call, or at least text, with the news. Sure, there are people in my life who are more than acquaintances but not quite good friends, but I don't feel the need to invest hours of my time—not to mention my mental health—scrolling through my feed to make sure I don't miss their posts. (And 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 inescapable part of social media.

And, 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 musings on the writing 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.

Option 1: You Decide to Close Your Social Media Accounts

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.)

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 privacy-oriented chat apps like Telegram.

If you belong to a group that uses the platform to make plans, share news, and so on, suggest moving the whole group somewhere else. Video platforms like Skype or Zoom, real-life meetups, and privacy-first chat apps are options.

Step 2 to Quitting Social Media: Download your data

Before you click "Close My Account" on any of these platforms, be sure to download any photos, posts, and other information you want to keep. Every site has its own procedures; for example, LinkedIn let me download my recommendations and some other data, but I had to copy and paste all my posts into a document by hand. (I'm sure there are apps to help with this, but I figured it would be easier to just do it manually and get it over with.)

Step 3 to Quitting Social Media: Start deleting

Here's how to close accounts on the most popular social media sites. These instructions are for deactivating accounts using your computer, not your other devices; the steps for deactivating accounts from the apps may be different.

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

Afraid to let go? Facebook, Instagram, Pinterest, and LinkedIn let you temporarily deactivate your account. (LinkedIn calls it "hibernating" your account.) When you start to follow the steps 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.

How to close your Facebook account

If you use Facebook to log in to apps or websites, you'll need to disconnect these first. Here are the steps:

1. Click on your profile picture.
2. Go to *Settings & Privacy*.
3. Select *Settings*.
4. Click on *Apps & Websites*; there, you can see a list of apps and sites with access to your Facebook account and remove the access.

Then, close your account:

1. Click on your profile picture.
2. Go to *Settings & Privacy*.
3. Select *Settings*.
4. If you see "Accounts Center" at the top left of the page, you can delete your account there. If "Accounts Center" is at the bottom left of the page, use Facebook Settings to delete your account.

Remember that Facebook owns WhatsApp as well! So if you want to wipe the slate clean, you may want to replace WhatsApp with Telegram or another privacy-oriented chat app.

How to close your Instagram account

Here are the instructions from Facebook's Help Center (since Facebook owns Instagram):

1. Go to the Delete Your Account page.
2. Choose an option from the dropdown menu for "Why do you want to delete [account name]?"
3. Re-enter your password.
4. Click *Delete [username]*.

How to close your LinkedIn account

LinkedIn provides a handy Close Account page. Done!

How to close your Twitter/X account

1. In the menu on the left, select *More*.
2. Choose *Settings and privacy*.
3. Under Your Account, click *Deactivate your account*.
4. Click *Deactivate*.
5. To confirm, enter your password and then click *Deactivate account*.

How to close your TikTok account

1. Click your profile picture on the upper right.
2. Choose *Settings*.
3. In the Manage Account tab, scroll down to the Account Control section and click *Delete*.
4. Click *Continue*.
5. Enter your password.
6. Click *Delete Account*.

How to close your Reddit account

When you delete your Reddit account, your posts and comments will remain there (but with the username hidden). If you want to delete your posts before deactivating your account, follow these steps:

1. Click on your profile icon on the upper right.
2. Select *Profile*.
3. Click *Posts*.
4. At the bottom of the post you want to delete, click the three-dot icon, then click the trash can to delete.
5. Repeat for each post.

These are the steps for deleting your comments:

1. Click on your profile icon on the upper right.
2. Select *Profile*.
3. Click *comments*.
4. At the bottom of the comment you want to delete, click the three-dot icon, then click the trash can to delete.

Finally, deactivate your account:

1. Log in to Reddit.
2. If you're a Reddit Premium member, cancel your Reddit Premium subscription first.
3. Visit your Account Settings.
4. Scroll down to the *Delete Account* section.
5. Click *Delete Account.*
6. If your account was created with your Google account or Apple ID, scroll down to the Connected Accounts section 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 Pinterest account

1. Click the “down” arrow on the upper right to open the menu.
2. Click *Settings*.
3. Click *Account management* from the left-side navigation.
4. Click *Delete account*.
5. Click *Continue*.
6. Select the reason you’re leaving.
7. Click *Send email* to receive an email to delete your account.
8. Check the email address associated with your Pinterest account to confirm you want to close your account.

If you belong to any platforms not listed here—like Mastodon, Nextdoor, Discord, Snapchat, Tumblr, or anything new that pops up—search for “how to delete [platform] account” to find instructions.

Option 2: You Want to Stay on Social Media

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.

Make your website your home base with POSSE

In some careers, building an audience is crucial; for example, artists, writers, and podcasters need to share their content to survive. However, social media platforms 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, how quickly even an OG social media platform can be destabilized.

Instead, share your thoughts, creations, and content on a platform you own. One method 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.

POSSE can be as simple as publishing posts on your own website and then manually copy-pasting them into the various social media 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; I've found the Wix website design platform to be the easiest and most intuitive, but there are many other options for quickly building a simple website as well.

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 are 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 an example of a POSSE; it's a response to the Verge article above. At the end of the post, author Tantek Çelik lists many, many tools and resources you can 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 how a POSSE site looks!
- 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 hashtags. Once you get through the learning curve, the experience should become much more streamlined and intuitive.

Choose your platform wisely

If social media is necessary for your job or business, and moving your content to your own website isn't feasible, think about which platforms are best for your purposes. Usually, those are the ones you like enough to really *work* at.

For instance, when I ran a content studio, we realized the vast majority of our clients came through LinkedIn. So rather than spreading ourselves thin trying to reach audiences through LinkedIn *and* Facebook, Twitter, Instagram, YouTube, TikTok, and the rest, we doubled down on LinkedIn. It worked so well that until I deleted my LinkedIn account—two years after I retired—I was still getting reach-outs from prospects!

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 by you). This works for any type of website you want to use only occasionally, but have trouble dragging your attention away from.

Another option is to use 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.

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 to communicate, I created an account using my first and middle names only, 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, a PO box, a throwaway phone number, etc.

Close the door (at least part way)

Some social platforms, like Instagram, let you create private profiles where people have to ask your permission to follow you. This is a great way to stay in touch with the people you want to stay in touch with while keeping random strangers from viewing your info. (Of course this doesn't keep the platform itself from tracking you or selling your data.)

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, 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 (and 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.

NOTES ON PART 4

Forum accounts I want to delete posts on/delete entirely:

Forum: _____ ☐ Delete posts ☐ Delete account ☐ Completed?

Forum: _____ ☐ Delete posts ☐ Delete account ☐ Completed?

Forum: _____ ☐ Delete posts ☐ Delete account ☐ Completed?

Forum: _____ ☐ Delete posts ☐ Delete account ☐ Completed?

Forum: _____ ☐ Delete posts ☐ Delete account ☐ Completed?

Sites I plan to remove my reviews from:

Site: _____ ☐ Completed?

Site: _____ ☐ Completed?

Site: _____ ☐ Completed?

Site: _____ ☐ Completed?

Site: _____ ☐ Completed?

Does social media really help me with my career? If so, what's the one platform that has the most impact?

How else can I accomplish the tasks I use social media for?

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

Do I need the information I get from social media?

Are the people on social media close enough friends for me to deal with the inconveniences of the platforms?

If I decide to use the POSSE method, what resources do I need to study/find/get?

What apps can I use to limit my time on social media?

What obstacles are keeping me from moving away from social media?

How can I overcome these obstacles?

To Do List:

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

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.

When we break these attention thieves' hold on us, not only do we shrink their power…we live richer lives by paying attention to what really matters to us.

CHAPTER 17: DON'T SURF IF YOU DON'T NEED TO

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 read 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 online ad companies know *too little* about them.)

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

How to opt out of the Digital Advertising Alliance

The Digital Advertising Alliance's YourAdChoices website has you enter your email or phone number to control how advertisers collect data associated with that address or number. This won't affect the ads you get via phone or email; the DAA's advertiser members actually identify you based on this info and know not to track you.

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 the 118 advertisers—but when I did it again in the fall of 2023, the system told me 23 of those advertisers were either serving personalized ads to my browser or their status was "unverified." 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

The Network Advertising Initiative is a similar industry group that lets you opt out of its member companies' browser-based advertising and matched advertising based on your email. It also gives instructions for opting out of interest-based ads on various mobile devices and internet-connected TVs.

Annihilate Ads Idea By...Blocking Them Outright

Of course, opting out of these networks doesn't stop ads—it only stops member companies from tracking you in order to serve you *personalized* ads. While this is good in itself, if you want to get rid of ads altogether, you'll need to install an ad-blocking browser extension.

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! These are a few popular ones:

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

Keep in mind, however, that some of your favorite online content is funded by advertising; you could always turn off the ad-blocker to allow ads from creators you want to support.

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.[25] 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, be prepared for the weather, identify a bird, track 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 comes with the bare minimum: phone, time, and text. You can use the online dashboard to add a few extras like a podcast player, music player, and turn-by-turn directions.

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 to allay boredom!

Option 2: Compromise with a Semi-Smart Phone

I do have to endure some inconveniences. For example, I borrow my partner's phone to deposit checks, and use my laptop to make Venmo payments, and look at the wall thermostat to see the temperature outside. When a business requires customers to scan a QR code for service, I march up to the front desk and ask for an alternative.

[25] www.pcmag.com/news/americans-check-their-phones-an-alarming-number-of-times-per-day

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.

I have to admit I'm trying so hard to love this phone, but while I like the distraction-free nature of it, I find texting and calls—the two things the phone is meant for—clunky, slow, and difficult. If that's a deal-breaker for you, try one of these semi-smart phones.

- WisePhone II looks like an actual smartphone and includes a camera—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.
- Ghost Phone Pro looks similar to WisePhone II and has many of the same features. In addition, many 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 phones are not compatible with all carriers; for example, my LightPhone doesn't work with Visible. Check the phone's website to see if you can stick with your current carrier.

Option 3: Install a Privacy-First Operating System

If you're more concerned about privacy than distraction, here's another option: 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 won't have to go without, say, your camera or a browser.

NOTES ON PART 5

What are the top reasons I find myself going online when I don't really need to? (Bored in a waiting room, want to look up a random fact, etc.)

What can I do instead of going online when I don't need to?

What are my top reasons for needing a smartphone?

What are the disadvantages to the way I use my smartphone?

What problems and inconveniences might come up if I get rid of my smartphone?

What are some ideas for dealing with those problems and inconveniences?

Smartphone alternatives to check out:

What if I try a dumb phone or semi-smart phone and it doesn't work out? What would I do then?

What obstacles are keeping me from moving from Google, Apple, Microsoft, and Amazon to more ethical alternatives?

How can I overcome these obstacles?

PART 6
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 Facebook earlier.)

These are the companies that use their power to lock us in to their products, kill off competitors, bombard us with ads, mistreat creators, and extract our data for corporate profit. Their massive privacy violations have turned us from living, breathing humans into dollar signs and data points.

In this section of the book, I'll give a quick critique of each company plus some solid alternatives to try.

CHAPTER 20: SAY GOODBYE TO GOOGLE

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

However: Google is 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. 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."[26] (See more on Google's monopolistic practices in Chapter 22: Say Arrivederci To Apple.)

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, but once you move to new platforms, they 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 again.

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

I researched and tested some of the suggested replacements on the NordVPN list as I went about getting rid of Google products. Here's what I ended up using, and how well these replacements worked. Like Google products, many of these alternatives are free and offer more space, features, and so on for a fee. If you're worried about making such a big switch, start with easier products like map or video services before tackling your email and browser.

[26] www.npr.org/2023/09/12/1198558372/doj-google-monopoly-antitrust-trial-search-engine
[27] nordvpn.com/blog/google-alternatives

EMAIL: Gmail → Proton Mail

For email, I chose Proton, which is a privacy-first email provider that also offers a calendar, password manager, VPN, and more. You can get an email address for free, or upgrade for more addresses, the ability to use your own domain, and other features. I've been happy with Proton except I find their email search to be slow and annoying. (Google can provide fast searches of your email content because they automatically claim access to your content—which is kind of why I opted for a non-Google email in the first place).

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 various 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 on my own domain: 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 as accounts with 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 reports, etc. to a masked address.

For the first few weeks, I occasionally caught important emails via the forwarding to Proton—for example, from people and businesses I neglected to alert to the change—and I switched them over to my new address. At this point, I mostly get nothing but spam at my main Gmail address.

I will actually be keeping the Gmail account alive in order to keep using Google Drive, at least for now (more below). But in time, it will be an unused shell of an email that shares nothing of importance with Google…and once I have my new system set up, I can delete it forever.

SEARCH: Google Search → DuckDuckGo or SimpleSearch

Rather than using Google Search, I use the privacy-oriented DuckDuckGo as my main search engine. 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 now I don't even give it a second thought.

If you decide to go with DuckDuckGo sure to change the default search engine in your 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. For iOS devices, follow these instructions; these are the steps for Android.

Can't do without the ease and personalization of Google Search? Simple Search is an extension for Firefox 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 wrench into Google's money-making machine.

(The extension is also supposed to be available for Chrome, but it looks like it's no longer available in the Chrome Web Store. Gee, I wonder why?)

CALENDAR: Google Calendar → Proton Calendar

My Proton account includes Proton Calendar, which works pretty much the same as Google Calendar. It's also easy to share with people who still use Google (and for them to share their Google calendars with me). The disadvantage is that while we can *share* and *view* events between the platforms, we can't *edit* events created in the other platforms.

PHOTOS: Google Photos → Ente

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

BROWSER: Google Chrome → Firefox

I chose Mozilla's Firefox browser in place of Google Chrome, and have been very happy with it. Mozilla is a non-profit emphasizing "privacy, openness, and a belief in the ability of the internet to enrich the lives of people." The Mozilla manifesto states, "Individuals' security and privacy on the internet are fundamental and must not be treated as optional."

I'd originally tested a couple of popular privacy browsers, and just didn't like the feel of them. If you'd like to try them yourself, they are Epic Privacy Browser and Brave.

If you change browsers, you'll also want to make your new choice the default browser for your phone, desktop computer, and other devices.

How to change the default web browser on iPhone, iPad, or iPod touch

1. Be sure you're running iOS 14 or later.
2. Make sure the browser you want is installed.
3. Go to Settings.
4. Scroll down until you find your new browser app.
5. Tap the app.
6. Tap Default Browser App.
7. Select a web browser to set it as the default. A check mark appears to confirm.

How to change the default web browser on your Mac desktop

In macOS Ventura or later:

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

In earlier versions of macOS:

1. Make sure the browser you want is installed.
2. From the Apple menu in the corner of your screen, choose *System Preferences*.
3. Click *General*.
4. Choose a web browser from the "Default web browser" menu.

How to change the default web browser on Android

1. Make sure the browser you want is installed.
2. Swipe down once or twice (depending on your phone).
3. Click the gear icon to open Settings.
4. Go to the Apps section.
5. Select *Default Apps* or *Choose Default Apps*.
6. Tap *Browser App* and select the browser you want to use.

How to change the default web browser on Windows 11

1. Make sure the browser you want is installed.
2. Click *Start*.
3. Click *Settings* in the pinned area.
4. Select *Apps*.
5. Select *Default apps.*
6. Click the arrow next to the browser you want to use, then click *Set default*.

Now, when you click on a link in, say, a text, it will open in the correct browser.

MAP: Google Maps → OsmAnd, HERE WeGo, or Paper Maps

While the NordVPN article offers alternatives to Google Maps, I don't use it enough to worry about a replacement. Looking over the list, I would personally go with OsmAnd, "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." And for the ultimate in privacy, don't forget paper maps! They still exist.

VIDEO: YouTube → Nebula and...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 ($5 per month or $50 per year) go to the creators.

Feeling FOMO about funny cat videos, or your favorite creator isn't on Nebula? 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 remain anonymous.

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 solid, secure alternatives.

CLOUD DOCUMENT EDITOR: Google Docs → Zoho Office

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, Note-book, Sheet, and Show products duplicate Google's popular office products and are free for individuals. You can get access to all of these through Zoho's Workspace, which offers 5GB of storage per user with up to five users, a 25MB attachment limit, and web access only.

CLOUD STORAGE: Google Drive → Proton Drive

I originally chose Box.com as my new cloud storage solution because it also 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's no easy way to automatically transfer the contents of your Google Drive. I tried various methods, none of which worked, and ended up laboriously downloading all my folders from Drive and uploading them into Box.

Then I discovered if you try to upload folders that contain subfolders, many of the subfolders are…empty. So my next task was to upload the individual subfolders one by one. This entire process took several days, on and off.

Second, 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.

My new plan is to move my files to Proton Drive for storage, and to use Zoho Office to create and edit documents in the cloud.

How to Stop Paying Google for Storage

Until I have a chance to implement my new plan, I decided to clear out my Drive files from many, many gigs to under 15 GB—not only to be able to use Drive for free, thereby withdrawing my dollars from Google, but also to minimize the amount of content I had sitting around in there.

If you'd like to reduce your storage to "free" levels, here are some tricks I used. (If you ever decide to move to another cloud storage service, at least you won't be paying for storage you don't need!)

Step 1: Decide what you need

What do you really need to have hanging around in Google Drive? For me, it was the important projects I've done in the past (such as books I've written and an app I developed), the last two years' worth of work, and projects I'm working on right now. The rest can be either somewhere else or gone from my life.

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 you don't need sucking up a lot of space? Trash them.

You can also click *Storage* and then *Clean Up Space* to see files in Drive, Google Photos, and Gmail that Google recommends you delete.

Step 3: Delete duplicate files

Duplicate files can be a huge culprit in sucking up your storage space. If you're on Android, Google provides an easy solution:

1. On your Android device, open *Files by Google*.
2. At the bottom, click *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 confirmation pop-up, tap *Move # file(s) to Trash*.

On a Mac? You're out of luck, at least for an easy solution. You can't even sort your files in alphabetical order on the Home page to easily suss out duplicates! I ended up using a free app; search for "duplicate file finder for Google Drive" to find tons of apps that can tackle this task. The free version will have some limitations, but it worked just well enough for me.

Step 4: Manually trash unneeded files

"Storage is cheap!" we say as we upload files willy-nilly. And now, if you're like me, you have hundreds or thousands of files in Drive you don't really need. For example, I had saved every single interview sound file and transcription from my 25-year career as a writer. Thankfully, I was very consistent in how I named files, so it wasn't too much of a chore to search for and delete all those files.

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? Look through your files—and be ruthless about it.

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 work on and share, transfer them to a Google Drive alternative such as Dropbox.

Step 6: Move files to an external hard drive

Anything I wanted to keep, but that didn't need to be in Drive, I downloaded to an external hard drive; the most important of these files I also keep on my laptop. I keep the hard drive in a fireproof safe and upload new files to it weekly.

Step 7: Empty the trash

Drive does this automatically every 30 days, but in the meantime the files there 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.

Turn off Google tracking

If you can't live without Google products, visit their Data & Privacy page, where you can 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.

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 21: 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' employees get screwed 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. (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 employees. Not only that, but people have been complaining that the products they're receiving from Amazon these days are either shoddy quality or straight-out counterfeits. I'm not talking 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![28]

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 broom is looking shabby? Just click and you can have a sparkling new one delivered to you today.

[28] pluralistic.net/2023/11/06/attention-rents/#consumer-welfare-queens

This habit doesn't do anyone any good. Instead, retrain yourself to wait a little longer for what you want. A smaller shop may have slower shipping, but that's OK—just learn to look ahead instead of racing to Amazon when you suddenly need something. You may have to wait a few days until you can actually visit a brick-and-mortar store for a plant stand or battery recharger, but this will give you the time to consider whether you really need it in the first place.

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 simply *you pre-paying for your own 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.[29] [The minimum has since been raised to $35.]

Stop Shopping at Amazon by...knowing thy enemy

Amazon doesn't just own Amazon. They also own companies like:

- Zappos
- Goodreads
- PillPack, a pharmacy
- One Medical (Don't love the idea of Amazon having our medical and pharma data!)
- Whole Foods
- Ring LLC (the smart doorbell company)
- Twitch, the streaming video and community platform for gamers
- iRobot, the makers of the Roomba vacuum, which Bloomberg called "a data collection machine that comes with a vacuum."[30]
- Audible, the audiobook store (we'll cover alternatives below)

[29] ibid.

[30] www.bloomberg.com/news/articles/2022-08-05/amazon-s-irobot-deal-is-about-roomba-s-data-collection

It can be hard to keep up, but if you know a business is owned by Amazon…look elsewhere.

Stop Shopping at Amazon by...looking around town

Next, explore your downtown and other local shopping centers. You may be surprised at what you can find there. 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 bake cakes, make funny 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. Because Amazon charges a premium to sell items on its site, this 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.

Stop Shopping at Amazon by...getting creative

Whenever you need something you know you can't find locally, see if you can find it through a smaller company online. When I wanted a unique gift for a friend who is an incredible host, I found hand-made serving trays created from recycled wine bottles at the Uncommon Goods website. I've also bought memorial trees, homemade brownies, and other goodies sold by smaller companies online.

Stop Shopping at Amazon by...visiting a big-box

Sometimes we just want to buy a pair of socks or some AA batteries and don't want to search all over town for them. Target, Walmart, Costco and other big-box stores, warehouse stores, and department stores aren't perfect, but they aren't anywhere near as bad as Amazon. (At least, not yet!)

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). You can snag 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 side, there are ways to keep reading without Amazon, Kindle, and Audible.

Instead of Amazon, try...using another e-reader

If you use a Kindle e-reader, you're stuck buying e-books from Amazon…unless you're OK with the costs of switching over to another service when your entire library is already on Kindle. This is because Amazon supports only its proprietary AZW e-book files, and doesn't allow you to sideload files in other formats. (Sideloading is installing software on a device without using the approved app store.)

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.

However, just because you switch e-readers doesn't mean all is lost! After all, you can always keep your old 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 your books frequently, but if you're mostly "once and done," you won't need to pull out the Kindle too often.

When my Kindle dies, my plan is to replace it with a different brand of e-reader, and to take comfort in the fact that I can always read my old books on the Kindle app. In the meantime, my books are coming from the library.

Ready to find a new e-reader? Here are some Kindle alternatives that let you read a variety of file formats.

- Kobo supports EPUB, EPUB3, PDF, MOBI, JPEG, GIF, PNG, BMP, TIFF, TXT, HTML, RTF, 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 the feature-comparison chart on their European website.
- PocketBook e-readers support PDF, EPUB, DjVu, FB2, FB2.zip, MOBI, DOCX, RTF, TXT, CHM, HTML (basic), CBZ, CBR, and CBT.
- NOOK e-readers from Barnes & Noble support EPUB and PDF file formats. This means you can buy e-books not just at Barnes & Noble but also from Kobo as well as smaller online booksellers (see below).

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 options 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:

- Smashwords, which lets young writers publish for free.
- Project Gutenberg, which mostly publishes works in the public domain and offers many free textbooks to high school and college students.
- e-books.com, one of the world's oldest and largest sellers of e-books.

And those are just sites that sell EPUB format books. The ability to read PDF, CBT, and other files gives you even more options.

Instead of Amazon, try...kicking Audible to the curb

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 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, and you receive one credit for $14.99 per month. You can add credits whenever you need them or buy audiobooks à la carte.
- 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 you can access unlimited works.
- Chirp lets you escape subscription fees; after all, why is it considered a given that we want to subscribe for audiobook access when we typically purchase e-books and physical books individually? Instead, with Chirp you can buy audiobooks individually at a steep discount.
- 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 dissing Audible.

Instead of Amazon, try...IRL bookstores

You think they're gone, but they're not. Scrappy 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 and Books-A-Million.

A search on Indiebound found nine independent bookstores in the city closest to my home. Just enter your zip code 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 solid discount.

Instead of Amazon, try...going to the library

Guess what? Many libraries lend not just physical 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 OverDrive and Libby apps. You can also browse your library's e-book catalog on its website. When you find an e-book you'd like to read, read the book's description page to see which apps the library uses to deliver the book.

CHAPTER 22: 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 about less than $100 million to operate.

Not only that, Apple has been accused of violating labor laws[31]—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.[32]

Leaving the Apple ecosystem can be a chore because the company and its products have made their way into every facet of our lives. Let’s dive into some ideas for making it happen.

Go Back to the Past

First, use the tips from earlier chapters to disengage from Apple:

- See Chapter 20: Say Goodbye To Google for suggestions on 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.

The products and ideas in these chapters will get you started on the path to an Apple-free life. Then, look to these alternatives to Apple software, music, and podcasts.

[31] www.cnn.com/2023/01/31/tech/apple-worker-rights-nlrb/index.html
[32] 9to5mac.com/2023/01/09/apple-privacy-tracking-lawsuit/

OPERATING SYSTEM: Mac → Linux or PureOS

If you feel up for the challenge, you can install Linux on your Mac and replace Mac's native applications with Linux equivalents, according to a Vice article on how to quit Apple, Microsoft, Google, Facebook, and Amazon. There are many free, open-source alternatives to various popular software programs you can use with Linux.[33]

Another option for the technically minded is PureOS, a "A free/libre and open source GNU/Linux operating system" that's "a fully-convergent, user friendly, secure and freedom respecting OS for your daily usage." This operating system has many software applications available, from games and video to graphics and office apps.

STREAMING MUSIC: Apple Music → resonate or SoundCloud

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."

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. 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.

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.

[33] www.vice.com/en/article/ev3qw7/how-to-quit-apple-microsoft-google-facebook-amazon

If that sounds like overkill, try Overcast, a simple but feature-rich podcast player for iPhone, iPad, and Apple Watch. Overcast is free, supported by small visual ads to promote podcasts, and you can optionally hide them for $10 per year.

WIRELESS EARBUDS: Apple AirPods → Sony WF-1000XM5

The product testing and review site Tom's Guide say these Sony wireless earbuds offer "outstanding sound, and one of the best user experiences around."[34]

CHAPTER 23: SAY MMM-BYE TO MICROSOFT

Everything you read above about Apple, Google, and Amazon? A lot of it applies to Microsoft as well. The company has been accused of war profiteering[35] and tax evasion[36]. It blocks apps on Windows 11 that allow users to choose the browser and search experience they want.[37]

Microsoft 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.[38]

I can't possibly cover all the ways Microsoft has helped to make the internet (and the world) a crappier place. But if the information above is enough for you to drop them like a hot rock, here are some ideas.

Go Backward

See Chapter 20: Say Goodbye To Google for suggestions on privacy-forward replacements for Edge Browser, Outlook email and calendar, Bing search, and other products. Then check out these alternatives for software suites and video game consoles.

---

[34] https://www.tomsguide.com/best-picks/best-apple-airpods-alternatives#section-best-airpods-alternative-overall
[35] www.theguardian.com/technology/2019/feb/22/microsoft-protest-us-army-augmented-reality-headsets
[36] boingboing.net/2020/01/22/clippy-dodges-taxes.html
[37] www.zdnet.com/article/microsoft-doubles-down-on-its-strategy-to-get-more-windows-11-users-on-edge
[38] en.wikipedia.org/wiki/Criticism_of_Microsoft

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. You can export your work in many different formats, including PDF. On the downside, LibreOffice doesn't offer mobile apps or online collaboration.

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 emulates the original Microsoft Xbox game console, enabling people to play their original Xbox games on Windows, macOS, and Linux systems." It supports almost all controllers, and you can connect up to four controllers 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 feeding Microsoft with your time, attention, and dollars, an emulator could be the way to go. Want to give it a try? The Xemu has a long, searchable list of Xbox games compatible with the emulator.

NOTES ON PART 6

Which Google, Apple, and Microsoft products do I want to stop using?

Alternative products to check out:

If my friends, family members, or work colleagues depend on products I want to stop using—for example, Google Drive or iCal—how can I still collaborate with them?

If I move to a new email provider, these are the people and businesses I'll need to alert:

Where can I get hard-copy books, ebooks, and audio books instead of Amazon?

What other products do I depend on Amazon for?

Where else can I find these products?

What obstacles are keeping me from moving from Google, Apple, Microsoft, and Amazon to better alternatives?

How can I overcome these obstacles?

To Do List:

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

Task: _____ Deadline: _____ ☐ Completed?

PART 7
LIVE YOUR LIFE

You've read through *Disengage*, maybe taken some notes, and perhaps even put some of the ideas into practice! Here's where we wrap it all up. This project will likely never be all wrapped up with a nice bow on top, but we can still make some great things happen.

Remember: 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 internet and the Big Tech companies that have claimed it as their own. As I researched, I learned about many products, technologies, and businesses I don't personally own, use, or frequent. I attempted to pull all this information together into this short guide.

I couldn't possibly cover every single action one might take to take back the internet—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 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 people publicly share what they buy and sell on Venmo so everyone can tell they collect unicorns and have a kid who plays soccer.

If there are any companies 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 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!

Keep Up the Good Fight

Thank you for reading *Disengage*. I hope this humble book helps you deprive hypercapitalist companies of at least a bit of your precious life.

If you'd like to get in touch, please reach out at LindaFormichelli.com. You can also visit to subscribe to ad-free, no-spam, rarely sent Punching Up Press emails. I'd love to grow Punching Up Press to a cooperative press that offers books by and for underdogs. If you subscribe, you'll learn about new books, opportunities for authors, and more.

FURTHER READING

These are the websites and books that inspired me as I researched and wrote this book.

WEBSITES

404 Media

A journalist-founded digital media company exploring the ways technology is shaping—and is shaped by—our world. They're focused on "investigative reports, longform features, blogs, and scoops about topics including: hacking, cybersecurity, cybercrime, sex, artificial intelligence, consumer rights, surveillance, privacy, and the democratization of the internet."

The Markup

The Markup challenges technology to serve the public good. Use the site's tools and blueprints to, for example, see how Twitter/X throttles competitors' sites and learn how to completely anonymize your phone.

Pluralistic

Daily links from Cory Doctorow.

Electronic Frontier Foundation

The leading nonprofit defending digital privacy, free speech, and innovation. I recommend these articles:

1. Debunking the Myth of "Anonymous" Data
2. To Address Online Harms, We Must Consider Privacy First

BOOKS

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power

By Shoshana Zuboff. The challenges to humanity posed by the digital future, the first detailed examination of the unprecedented form of power called “surveillance capitalism,” and the quest by powerful corporations to predict and control our behavior.

Chokepoint Capitalism

By Cory Doctorow and Rebecca Giblin. A call to action for the creative class and labor movement to rally against the power of Big Tech and Big Media.

Survival of the Richest: Escape Fantasies of the Tech Billionaires

By Douglas Rushkoff. Five mysterious billionaires summoned theorist Douglas Rushkoff to a desert resort for a private talk. The topic? How to survive the “Event”: the societal catastrophe they know is coming. Rushkoff came to understand that these men were under the influence of The Mindset, a Silicon Valley–style certainty that they and their cohort can break the laws of physics, economics, and morality to escape a disaster of their own making—as long as they have enough money and the right technology. [Note from Linda: Yes, this is nonfiction!]

How to Do Nothing: Resisting the Attention Economy

By Jenny Odell. In a world where addictive technology is designed to buy and sell our attention, and our value is determined by our 24/7 data productivity, it can seem impossible to escape. But in this inspiring field guide to dropping out of the attention economy, artist and critic Jenny Odell shows us how we can still win back our lives.

Odell sees our attention as the most precious—and overdrawn—resource we have. And we must actively and continuously choose how we use it. We might not spend it on things that capitalism has deemed important … but once we can start paying a new kind of attention, she writes, we can undertake bolder forms of political action, reimagine humankind’s role in the environment, and arrive at more meaningful understandings of happiness and progress.

Extreme Privacy: What It Takes to Disappear

By Michael Bazzell. This textbook [...] provides explicit details of every step he takes to make someone completely disappear, including document templates and a chronological order of events. The information shared in this volume is based on real experiences with his actual clients, and is unlike any content ever released in his other books. [Note from Linda: I haven't read this book because it's pretty expensive—but this 500-page tome looks like it covers some of what I write about in this book, and then goes much, much further for those who are willing to put up with major inconveniences to completely disappear from the internet (and elsewhere). Unfortunately, it's only available on Amazon.]