66 Ways to Protect Your Privacy Right Now

Ah, the joys of the connected life: opportunities to engage with global communities, be educated and entertained, and shop with ease. But these go hand in glove with intrusions from marketers and threats from criminals. The tips on the following pages, compiled with input from dozens of security experts, will help you take control. Start on page 28.
When I was growing up in the 1980s, my parents would occasionally take my brother and me for a special treat: an evening spent browsing for software at a local computer store.

We would wander among the aisles of shiny, shrink-wrapped boxes, lobbying our parents to buy us games such as the geography spy mystery “Where in the World Is Carmen Sandiego?”, which cost about $40 a pop.

Flash-forward nearly 30 years, and my own kids can’t believe I ever paid so much for a computer game. Most software packages—from games to productivity apps to health-tracking apps—are free.

There’s only one catch: We pay for all this software with a new currency, our personal data. Whenever we download an app, visit a website, watch a smart TV, use free WiFi, or partake of most of the joys of the information age, we agree to give up previously unimaginable amounts of personal data.

The shift toward data as currency began somewhat innocuously. At first, we simply accepted ads targeted to our search queries. But now, a decade later, the trade-offs have become more extreme. We implicitly agree to have our movements followed both virtually, as we browse the web, and physically, as our phones transmit our locations. We agree to have our interests cataloged and analyzed. We agree to have the

But first, read what investigative reporter Julia Angwin learned in her own quest to boost her privacy.
content of our emails scanned. We agree to have our friends identified and analyzed in “social graphs.” We agree to have our images stored, shared, and tagged and our faces analyzed to help companies perfect their facial recognition tools. We agree to have our voices analyzed, our fingerprints scanned, and soon enough, the iris patterns of our eyes stored in vast, remote databases.

Theoretically, we could read all the fine print in the “terms and conditions” and “privacy policies” foisted on us and refuse to use products that track us egregiously. But who has time to do that? In a 2016 experiment by researchers at Toronto’s York University and the University of Connecticut, 74 percent of people who joined a fictitious social network skipped reading the privacy policy altogether. And those who opened the terms and conditions must not have read them very carefully—because all of them agreed to give up their firstborn child to the social network.

In fact, failing to read privacy policies is perfectly rational. In 2008, Carnegie Mellon researchers estimated that it would take an average individual 154 hours to skim the privacy policies for the approximately 1,462 websites they encountered each year. In terms of wages and lost time, that would amount to $2,226 per person.

Even if we read all those policies, we still couldn’t accurately weigh our privacy trade-offs. Our data is a currency that we trade for services, but we don’t really know what the data will cost us in the future. Could it keep us from landing a job? Rob us of a good deal on insurance? Get us thrown in jail? It’s impossible to say.

All we know for sure is that it seems like it would cost a lot of time and energy now to try to keep our data from costing us even more in the future. No wonder most people feel overwhelmed by the task.

**Paging Ida Tarbell**

One day in 2012, I was on a city bus talking to a friend about how hopeless privacy trade-offs can seem. She asked: “Is it hopeless because no one cares? Or is it truly hopeless?” In a flash, I realized that I didn’t know the answer. I hadn’t ever really tried to protect my privacy because I assumed it would be too difficult.

So I began a privacy experiment. For a year I sought to protect my data as much as possible while continuing to remain connected to the internet, my phone and my friends, and all the joys of the information age.

What I found was that protecting my privacy wasn’t as difficult as I thought. There were plenty of steps—I or anyone—could take that were simple, cheap, and effective. And most important, my actions gave me a feeling of reclaiming control over the technology invading every corner of my life.

I started with the basics of computer security—essentially, locking the doors of my digital home. I updated all my software so I wasn’t vulnerable to criminals who might exploit flaws in old versions. I deleted free applications that I was no longer using that could be stealing my data. I installed software and adjusted the privacy settings on my web browser to block the most common types of tracking used by advertisers. I purchased software to help me generate and manage strong passwords. I covered my laptop camera with tape so that hackers couldn’t see anything if they took control of it remotely (which unfortunately is easy for them to do).

Once I had secured most of the entry points to my digital domain, I began trying to reclaim my data from as many places as possible. I took some big steps, and I realize not everyone will want to follow my lead.

"I’ve called the bluff of those who believe privacy is dead. In fact, there’s a lot you can do."

First, I stopped using the social networks LinkedIn and Facebook. Surprisingly, I didn’t miss them much—I discovered that I preferred staying in touch with friends through phone calls and visits. Next, I decided to break up with Google. The company had famously promised not to be “evil” in its corporate motto. But when I checked my account’s privacy dashboard, I saw that Google had more intimate information about me than my closest friends and family. Google’s search history revealed that I often browsed for shoes when I was stressed out on tight work deadlines. Google Maps recalled all the trips I had taken, foreign and domestic, along with my precise routes. And I already knew that Google’s Gmail recorded the fact that I emailed my close girlfriends more than my husband.

I started by abandoning Google’s admittedly excellent search engine. I began searching on the website DuckDuckGo.com, which doesn’t track its users. It makes money the quaint old-fashioned way, by showing so-called “contextual” ads related to the search query rather than “behavioral” ads that track users across websites.

Replacing Gmail with a service that promised not to scan my personal correspondence was more expensive. I gave up both Gmail and Google Docs, and ended up paying about $200 per year for an encrypted cloud storage system—and then invested $100 for a hard drive to store my emails at home. I was starting to feel like a data survivalist, stockpiling terabytes of personal info.

Yet all these digital barriers didn’t help me hide the details of my offline life—whom I had coffee with, where I saw movies, whom I emailed. So I pulled a real Jason Bourne move: I created a fake identity. (Yes, it is legal to maintain an alias if it’s not used for fraud.) I began using the name Ida Tarbell, after the turn-of-the-century muckraker who revealed Standard Oil's
abuse of its monopoly power. I set up Ida with a credit card (linked to my account), an email address, an Amazon account, a postal address, a cell phone, and even a few social media accounts.

Even though Ida was the thinnest of disguises—any decent investigator could link her to me—I found using her as an alias to be incredibly satisfying. I loved booking a restaurant reservation under her name and being greeted as Ida. I loved ordering books about the history of the National Security Agency from her account rather than mine. I loved using her name to sign up for stupid online games that I was embarrassed to be caught playing.

Ida is my homage to the fleeting pleasures of the past, a past anyone over the age of 40 can recall but younger people may find hard to grasp. Back when buying a video game or a frivolous magazine or a drink with an old boyfriend didn’t create a data trail to be stored, scrutinized, and analyzed for generations to come. Using Ida’s name empowers me by restoring anonymity to everyday life.

**Privacy as Mindfulness**

Armed with my tracker-blocking software, my secure passwords—and, of course, Ida—I believe I’ve called the bluff of those who claim that privacy is dead. In fact, there’s a lot you can do.

And yet.

The multibillion-dollar trade in personal data—what’s often called the surveillance-industrial complex—continues to expand. I’ve had wins in my personal battles, and so have many others. But a larger win would be a shift in the balance of power between the data collectors and the rest of us.

You see, I wouldn’t mind some of my behavior being tracked if I knew the data wasn’t going to end up denying me a job or a loan one day. If I knew that I could successfully dispute it in court. If I didn’t constantly have to sign unconscionable contracts allowing companies to use my data however they liked. If I knew that the data collectors would protect my information from being hacked. If I knew that my children’s future wouldn’t be forever marked by an idiotic video they posted when they were 8. If I knew that I could indulge in ephemeral, innocent joys without leaving a permanent record.

But I don’t have any of those guarantees today. In Europe, companies that collect personal data are required to give people access to their data, the ability to dispute it, and in some cases, the right to remove it. But the United States has no such laws. And the companies themselves don’t seem to be leading the way.

So until I can be assured how my data will be used in the future, I’m reluctant to employ it as a currency to buy services. Instead I choose to pay whenever possible with dollars, with my effort, and with my time. Three years after my experiment was supposed to end, I still do most of my privacy-protecting moves. I secure my computer. I block tracking. I reclaim my data when I can. I hoard my data at home. And I delight in using my fake identities. (Yes, I have a few others, too.)

Despite its hassles, I’ve grown to like the practice of privacy. To me, it’s another form of mindfulness. Even though I know my victories are incomplete, they give me a sense of control over the technology that is encroaching on my life. Each new act of resistance gives me strength to imagine a better world, one where we have some assurances about how our data is used. It’s not that hard. And I hope that others find a few acts of resistance that work for them, too.

---

**Julia Angwin is an award-winning senior reporter at ProPublica who covers technology and surveillance. She is also the author of “Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance” (Times Books, 2014).**

Continued on next page