

PRIVACY IN AMERICA

The Starter Guide

What They Already Know About You — And How to Take It Back

The United States is the only major democracy with no comprehensive federal privacy law. That means your rights depend on your zip code, and the companies harvesting your life are counting on you never finding out. This guide walks you through every threat covered in the book *Privacy in America* — and gives you the first moves to fight back, starting today.

MITCH JACKSON

California trial lawyer · Four decades fighting for people whose rights were violated

Get a FREE PDF version of the book with your monthly, annual and founding membership)

21 chapters. Real stories. More about the book, the law, plainly. And a 30-minute plan for your whole family at mitch-jackson.com/privacy

START HERE

They Already Have Everything

Think about an ordinary Tuesday. Your phone sent your location to advertisers. Your car logged your route, your speed, and whether you buckled your seatbelt. Your search queries became data points in a profile tied to your name. If a stranger followed you all day writing down every place you went and every question you typed, you would call the police. The digital version of that surveillance happens every single day, and the companies doing it already have a device in your pocket doing the work for them.

You did not agree to be the product. You do not have to remain the product. This guide is your map. Each section below points to a chapter in the book where the full story, and the full action plan, lives.

PART ONE · THE SYSTEM BUILT TO FAIL YOU

CH. 1 The Privacy You Trust Isn't Real

One hundred and forty-four countries protect their citizens with a national privacy law. The United States does not. Two people in two different states can download the same app, hand over the same data, suffer the same breach — and only one has any legal recourse. The only difference is their address. **Chapter 1 reveals why Congress has killed every privacy bill for 25 years, and the one browser setting that already carries legal force.**

84% of Americans

support stricter federal privacy laws — one of the most bipartisan issues in the country. Industry spent over \$250 million in a single year to make sure it never happened.

CH. 2 Data Brokers — They Sold You for a Penny

A company you have never heard of owns a file on you: your address, your income, your health conditions, your political leanings, and everywhere your phone has traveled this year. It will sell that file for less than a dollar. This industry has a body count, from a stalking victim in 1999 to an assassinated state lawmaker in 2025. **Chapter 2 names the brokers, shows what your life costs to buy, and walks you through California's new DROP deletion tool.**

CH. 20 You Clicked Agree and Signed Away Your Rights

In one study, 98% of people agreed to a consent form granting the company naming rights to their firstborn child. The whole system of “I Agree” is a performance: cookie banners engineered to exhaust you, privacy policies averaging 7,000 words, “dark patterns” built by teams of psychologists to steer your choice before you ever see the screen. **Chapter 20 teaches you to spot the manipulation in seconds.**

DO THIS TODAY

- › **Turn on Global Privacy Control.** Use Brave, DuckDuckGo, or Firefox (or add the EFF's Privacy Badger to Chrome). One setting tells every site “do not sell my data” — and in 12 states it is legally binding.
- › **If you live in California, register at DROP.** Go to privacy.ca.gov/drop. One free request reaches every registered data broker in the state. It takes ten minutes.
- › **When a banner appears, click the small gray option.** The big bright button is almost always the one that surrenders your data.

Your Phone, Your Home, Your Car

CH. 3 Your Phone Sends Your Location 747 Times a Day

More than once every two minutes during your waking hours, an invisible auction fires inside your phone and broadcasts your GPS coordinates to companies you have never heard of. A weather app, a game, a prayer app, buried code records where you sleep, worship, and see your doctor. In January 2025 a single breach dumped the precise locations of millions of Americans onto the open internet. **Chapter 3 includes a five-minute privacy reset for iPhone and Android.**

747 times a day

Your physical location is broadcast to the advertising system — 294 billion broadcasts a day in the U.S. alone, a system one regulator called “the biggest data breach ever recorded.”

CH. 4 Your House Is a 24/7 Recording Studio

The smart speaker, the doorbell camera, the TV on your wall, sold as convenience, built as surveillance. Companies have been caught letting employees watch women in their bedrooms, keeping 800,000 children's voice recordings after parents demanded deletion, and capturing what is on your screen twice every second to sell to advertisers. **Chapter 4 shows you which devices keep your data inside your own walls.**

CH. 5 That Car Knows More About You Than Your Spouse Does

A connected car generates 25 gigabytes an hour — your location, speed, hard braking, even whether you buckled up — and sells it to insurers and brokers. Drivers saw premiums jump after data they never knew they shared. Abusers have tracked survivors through their own vehicles. Every one of 25 car brands failed a privacy review. **Chapter 5 tells you how to pull the report your automaker built on you.**

DO THIS TODAY

- › **Kill your phone's advertising ID.** iPhone: Settings › Privacy & Security › Tracking — turn off “Allow Apps to Request to Track.” Android: Settings › Privacy › Ads — “Delete advertising ID.” This breaks the master key brokers use to follow you.
- › **Set apps to approximate location.** Most apps don't need your exact GPS. Switch off “Precise Location” for everything but navigation.
- › **Audit your car.** Open your vehicle's app and disable data-sharing/driving-behavior features. Request your free LexisNexis (1-888-497-0011) and Verisk reports to see what they've collected.

Surveillance You Can't Reset

CH. 6 Once Someone Captures Your Face and Voice, No Password Reset Can Save You

If your credit card is stolen, the bank mails a new one. You cannot request a new face. Clearview AI scraped 50 billion photos. Cameras scan you at airports, stadiums, and stores. And the system misidentifies people of color, women, and the elderly far more often, a Tennessee grandmother spent 108 days in jail over a false match. **Chapter 6 covers your right to opt out of the face scan and the family “code word” that defeats voice-cloning scams.**

CH. 7 Protesting, ICE, Police, and Surveillance

Predator drones over American cities. Facial-recognition apps scanning faces on public streets. License plates run through a national database the moment you park near a march. The tools the FBI needed half a million case files to deploy against the civil rights movement now fit inside one app on an agent's phone. **Chapter 7 lays out your rights and the exact steps to take before, during, and after a protest.**

CH. 18 Your Data Is Being Sold to the Government

The government needs a warrant to make your carrier hand over your location. So instead it buys the same data from a broker — no judge, no probable cause. The FBI, ICE, the IRS, the NSA, and the DEA are all customers. One DHS attorney compared buying your movements to “buying a widget.” **Chapter 18 explains the loophole and the bipartisan bill written to close it.**

\$1 billion ceiling

ICE's 2026 data-and-analytics agreement with a single surveillance contractor. Your tax dollars are financing the surveillance of you.

DO THIS TODAY

- › **At the airport, opt out.** Tell the TSA officer “I'd like to opt out of the face scan” before the photo. You don't owe a reason. Children under 18 aren't photographed.
- › **Before a protest, switch off biometrics.** Disable Face ID / Touch ID and use a strong passcode, a passcode in your mind has stronger constitutional protection than your face or fingerprint. Use Signal for sensitive messages.
- › **Cut the source.** Deny precise-location access to any app that doesn't truly need it. Less data on your phone means less data for brokers — and the government — to buy.

Deepfakes, AI Fraud, and the Secrets You Type

CH. 8 Deepfakes — When Your Eyes Lie to You

The rule you grew up with — if you saw it or heard it, you could trust it — is breaking apart. A few seconds of your voice scraped from social media is enough to make you say things you never said. A fake doesn't need to be perfect. It only needs to survive your first emotional reaction. **Chapter 8 replaces “seeing is believing” with the verification habits that keep families safe.**

CH. 9 AI Turned Fraud Into a \$12.5 Billion Weapon

A mother heard her daughter sobbing on the phone, begging for help. It was a machine. Voice cloning needs as little as three seconds of audio. Finance workers wired \$25.6 million after a video call where every “colleague” was a deepfake. Romance bots now run months-long relationships with no human behind them. **Chapter 9 gives you a family defense plan you can build in 30 minutes.**

\$12.5 billion

Lost by Americans to fraud in 2024 — a 25% jump in one year. Experian calls 2026 a “tipping point.” The figure is the floor, not the ceiling.

CH. 10 AI Chatbots — Your Secrets Are Training Their Data

Every major AI company trains on your conversations by default. Human reviewers read transcripts. Your words are kept for weeks, years, or forever. And there is no legal privilege, a federal judge ruled in 2026 that what you tell a chatbot can be seized and used against you. **Chapter 10 shows you the off switch on every major platform and what to never type.**

CH. 11 Once AI Takes Your Data You Can't Get It Back

Researchers found passports, credit cards, and medical photos inside the data sets used to build today's AI — scraped from people who never consented. The hard truth: once your data trains a model, removing it is, for all practical purposes, impossible. It went in through a one-way door. **Chapter 11 shows you how to check if your images were taken, and how to limit the damage going forward.**

DO THIS TODAY

- › **Set a family code word tonight.** A secret phrase that must be spoken in any emergency call asking for money. If you can't get it, hang up and call back on a number you already have.
- › **Turn off chatbot training.** On each AI tool, open Settings › Data Controls/Privacy and disable model training. Never paste SSNs, medical details, passwords, or legal strategy. Treat every chat like a postcard.
- › **Freeze your credit at all three bureaus.** Equifax, Experian, TransUnion. It's free, it's permanent, and it stops criminals from opening accounts in your name.

Your Health, Your DNA, Your Kids

CH. 12 HIPAA Won't Save Your Health Data

Eight in ten Americans believe their health apps are protected by HIPAA. They are not. Your therapy app, your period tracker, the wearable on your wrist, all of it sits outside the law. One therapy platform uploaded seven million clients' emails to Facebook. Brokers sell mental-health profiles for a nickel a person. **Chapter 12 shows you how to audit every health app on your phone.**

CH. 13 Your Reproductive Data Isn't Private

A journalist bought a week of location data for 600 Planned Parenthood clinics for \$160. Women have been prosecuted using their own search history and text messages. The one federal rule protecting reproductive records lasted eleven months before a court struck it down. **Chapter 13 names the safest apps and the steps to take before any clinic visit.**

CH. 14 They Sold Your DNA Without Asking You

When 23andMe went bankrupt, the genetic data of 15 million people became an asset in a corporate fire sale. A hacker once offered stolen profiles for a dollar each. Your DNA never changes, and it isn't yours alone, your spit in a tube exposes your parents, your siblings, your children, and cousins you've never met. **Chapter 14 walks you through deleting your data and destroying your sample.**

CH. 15 Your Kids Are Being Watched

By age 13, an estimated 72,000 data points have been collected about a child. School monitoring software flags student artwork as a crime, outs LGBTQ kids, and sends police to homes over after-hours searches, with little proof any of it works. A single breach exposed 62 million student records. **Chapter 15 tells you exactly what to ask your school, and how to teach kids what no law will.**

51 times more likely

Children are 51 times more likely than adults to have their identity stolen — and it often goes undetected for over a decade. Freeze your child's credit today.

DO THIS TODAY

- › **Use a separate email for health apps.** It keeps your health profile from being stitched to the rest of your digital identity, and turn on any “anonymous” or local-storage mode the app offers.
- › **Delete your DNA data.** Log in, download a copy first, then permanently delete your data and request destruction of your physical sample.
- › **Freeze your child's credit.** At all three bureaus. There is no legitimate reason a child needs an open credit file — and it blocks the most common form of child identity theft.

Your Number, the Breach Letter, and the Price You Pay

CH. 16 It's Your Phone Number and It's Putting Everything at Risk

A criminal called a carrier, pretended to be a Silicon Valley engineer, and moved his number to a new SIM card. Twenty minutes later, a million dollars — his daughters' college fund — was gone. Your phone number has quietly become the master key to your bank, your email, and your retirement accounts. **Chapter 16 shows you the free carrier locks almost nobody turns on.**

CH. 17 Ransomware and Data Breaches Can Destroy Your Life

Eighty percent of Americans got a breach letter last year. The largest healthcare breach in history, 192.7 million people, two of every three Americans, happened because one server was missing a single security checkbox. Your stolen Social Security number never expires and keeps generating new victims for years. **Chapter 17 lists every bureau to freeze, including the ones most people have never heard of.**

CH. 19 Algorithms Are Using Your Data to Overcharge You

Two shoppers, same store, same Tuesday, same cart — different prices. An algorithm reads your data, estimates what you'll tolerate, and charges you that. The same logic raised your rent and feeds secret files that decide whether you get an apartment, a job, or a fair insurance rate. One in five of those files contains an error. **Chapter 19 shows you how to pull your hidden files and dispute what's wrong.**

\$5.21

What the average person received when Equifax lost 147 million Social Security numbers. The legal system pays you pennies, which is why protecting yourself can't wait for it.

DO THIS TODAY

- › **Lock your phone number.** In your carrier's app, turn on SIM Protection and Port-Out / Number Lock, and set a strong account PIN. Then move your key accounts off SMS codes to a passkey, authenticator app, or hardware key.
- › **Check what's already exposed.** Search your email at haveibeenpwned.com, stop reusing passwords, and turn on multi-factor authentication everywhere.
- › **Pull your hidden files.** Get your free reports from AnnualCreditReport.com plus specialty agencies (ChexSystems, LexisNexis, The Work Number). Dispute every error by certified mail.

Your Privacy in 30 Minutes

Nobody is going to protect your data for you. The companies collecting it have no reason to stop, and Congress has failed to act for decades. The good news: the most effective tools are free, and you can start right now. **Chapter 21 is the full plan for you and your family. Here is where to begin.**

DO THIS TODAY

- › **Audit your phone (10 min).** Turn off app tracking, delete your advertising ID, set apps to approximate location, and run iPhone's Safety Check or Android's Privacy Dashboard.
- › **Switch your browser (2 min).** Move to Brave, Firefox, or DuckDuckGo and turn on Global Privacy Control. Stop letting Chrome track you by default.
- › **Freeze your credit (10 min).** Equifax, Experian, and TransUnion — plus Innovis, ChexSystems, NCTUE, and LexisNexis. Free, permanent, no effect on your score.
- › **Upgrade your logins (5 min).** Replace text-message codes with a passkey or hardware key on your bank, email, and investment accounts.
- › **Have the conversation (3 min).** Set a family code word. Tell your parents that any urgent call demanding money is almost certainly a scam.

This Is Not About Having Something to Hide

Saying you don't care about privacy because you have nothing to hide is like saying you don't care about free speech because you have nothing to say. Privacy is the space where you think freely, disagree openly, and make personal decisions without someone else owning the record. **You deserve to know what's happening to your information. And you deserve a guide who tells you the truth in plain language.**

READ THE WHOLE STORY — FREE

Privacy in America

Twenty-one chapters. Real stories. The law explained plainly. Each one ends with concrete steps you can take right now — and the final chapter gives you a 30-minute privacy plan for your whole family. The book is free, online, and updated the moment new laws and cases drop. A free PDF of the book is available to all monthly, annual and founding members.

More info about the book: mitch-jackson.com/privacy

Your privacy is worth the fight — and so are you.