Taking Back Your Privacy: A Practical Guide for Non-Technical People

Taking Back Your Privacy: A Practical Guide for Non-Technical People

> Written with the help of Claude AI. This is not legal advice.
> *Based on privacy principles from the Electronic Frontier Foundation*

The modern internet runs on surveillance. Every app on your phone tracks your location. Social media companies monetize your personal data. Data brokers compile dossiers on millions of people without their knowledge. For someone facing stalking, harassment, or domestic violence, this surveillance infrastructure becomes a weapon.

This guide translates technical privacy advice into actionable steps for people without cybersecurity expertise. It draws heavily from the Electronic Frontier Foundation's Surveillance Self-Defense project, research from Privacy Rights Clearinghouse, and resources from the National Network to End Domestic Violence.

Privacy isn't about having something to hide. As the EFF states in their foundational work: "Privacy is about protecting your right to be yourself." It's about control over your information in a world where that control has been systematically stripped away.

Understanding Your Threat Model

The EFF's Surveillance Self-Defense guide begins with a critical question: "What are you protecting against?" For most people reading this, the answer isn't government surveillance or corporate tracking. It's someone specific who wants to find you or monitor you.

The Coalition Against Stalkerware identifies the most dangerous types of information: your home address, which allows physical access; your daily routines, which create predictability; your phone number, enabling direct contact; photos with location data; and vehicle information that can be tracked.

According to the National Network to End Domestic Violence's 2023 Technology Safety Survey, 71% of domestic violence programs reported that abusers tracked survivors through social media, and 54% reported tracking through location-sharing features on phones. This isn't theoretical. The infrastructure of modern technology actively enables abuse.

But as the EFF notes repeatedly throughout their work, privacy doesn't require going off the grid. It requires understanding which information creates vulnerability and systematically limiting exposure.

Mobile Phones: Your Primary Vulnerability

The EFF's research on mobile phone surveillance is unequivocal: smartphones are designed to track location constantly, and this data is shared far more widely than users realize. As their Street-Level Surveillance project documents, location data reveals where you sleep (your home), where you work, what doctor you visit, what religious services you attend, and what political activities you engage in.

This data isn't private. App developers share it with advertising companies, data brokers purchase and resell it, and law enforcement can access it through various legal mechanisms. In stalking contexts, location data becomes a roadmap to your life.

Disabling Location Tracking

The first step is turning off location services for apps that don't require it. On iOS devices, navigate to Settings > Privacy & Security > Location Services and review each app's permissions. On Android, access Settings > Location > App Permissions. Social media applications—Facebook, Instagram, Twitter/X, Snapchat, TikTok—are particularly aggressive about location collection and should be set to "Never" unless absolutely necessary.

Beyond current tracking, your phone maintains a detailed history. Apple's "Significant Locations" feature and Google's "Timeline" create comprehensive records of everywhere you've been. The EFF's guide on mobile security emphasizes that this history can be subpoenaed, hacked, or accessed by anyone who gains physical access to your unlocked device. Delete this history and disable the feature.

On an iPhone, you'll find this under Settings, Privacy & Security, Location Services, then scroll down to System Services and look for Significant Locations. Turn it off and clear the history. On Android, you'll need to open Google Maps, tap your profile picture, go to Your Timeline, access the settings, and disable Location History. While you're there, delete the existing timeline data.

Device Security Fundamentals

According to the EFF's security recommendations, particularly those developed for protesters but applicable to anyone facing threats, a strong device passcode is the last line of defense. Six-digit PINs are minimum; alphanumeric passphrases are better. Biometric authentication (Face ID, fingerprint) should be enabled alongside, not instead of, strong passcodes. Auto-lock should be set to 30-60 seconds maximum.

Research from Johns Hopkins University's Information Security Institute found that most people significantly underestimate how much sensitive information their phones contain. An unlocked phone provides access to messages, photos, emails, banking apps, location history, and saved passwords—essentially a complete map of someone's digital life.

Application Permissions

Apps routinely request permissions far beyond what they need to function. A 2022 study by the International Computer Science Institute found that 88% of Android apps requested at least one dangerous permission, and many requested permissions unrelated to their stated functionality.

Review permissions monthly. On iOS: Settings > Privacy & Security, then review each category (Camera, Microphone, Contacts, Photos). On Android: Settings > Privacy > Permission Manager. If an app doesn't need a permission to function, deny it.

Social Media: Surveillance by Design

Social media platforms operate on what Harvard Business School professor Shoshana Zuboff calls "surveillance capitalism"—business models built on extracting and monetizing personal data. As the EFF stated in their 2023 analysis: "Social media companies have built their business models on surveillance. Your posts, your likes, your friends, your location—all of it is data to be monetized."

This creates a fundamental conflict. Platforms maximize profit by encouraging maximum sharing. But for someone concerned with safety, every post is a potential vulnerability.

The Case for Abstention

The most secure social media strategy is non-participation. The National Network to End Domestic Violence's Safety Net Project recommends that survivors of technology-enabled abuse consider deactivating or deleting social media accounts entirely. Information you don't share cannot be exploited.

Privacy Configuration

For those who continue using social media, the EFF's Surveillance Self-Defense module on social networks provides detailed configuration guidance. All accounts should be set to maximum privacy: on Facebook, Settings > Privacy > Future Posts should be "Friends Only"; Instagram requires enabling Private Account; Twitter/X offers tweet protection; TikTok provides private account options.

Location features must be comprehensively disabled. Check-ins broadcast real-time location. Location tags attach GPS coordinates to posts. "Nearby friends" features reveal when you're in proximity to others. All should be turned off.

Tag review is critical because it controls what others can reveal about you. Facebook allows Settings > Timeline and Tagging > Review tags before they appear on your timeline. Instagram offers Privacy > Tags > Manual approval. Even perfect personal privacy discipline can be undermined by friends and family who tag you in photos or posts.

Content Considerations

The EFF's "Think Before You Share" guidance emphasizes that once information is posted, you've lost control of it. Screenshots exist permanently. Even deleted posts may have been saved or shared.

Research from Carnegie Mellon University's CyLab found that users consistently underestimate how much can be inferred from seemingly innocuous social media posts. A study published in the Proceedings of the National Academy of Sciences demonstrated that location could be accurately predicted from social media posts even when location services were disabled, based solely on visual content and contextual clues.

Real-time location posts ("At Starbucks now!"), vacation announcements before or during travel, routine-revealing content ("Monday morning coffee run!"), photos showing home exteriors or address numbers, images containing license plates, workplace location information, and identifying details about children's schools all create specific vulnerabilities.

Secondary Disclosure

Privacy Rights Clearinghouse identifies "secondary disclosure"—when your privacy is compromised by others' posts—as one of the most common failure points. Family members post about visiting you and mention your city. Partners tag you at restaurants. Friends share group photos with your face visible.

The solution requires direct conversation with your circle. Research from the Pew Research Center on social media and privacy found that 64% of Americans have experienced privacy problems due to others posting information about them. Explaining that you need privacy for safety reasons and requesting specific behavioral changes is necessary.

Photo Metadata: The Invisible Exposure

Every smartphone photo embeds metadata—information about when, where, and how the image was created. As the EFF's guide on metadata states: "Metadata is data about data... and it can reveal far more than you intended to share."

Understanding EXIF Data

Standard photo metadata (EXIF data) includes GPS coordinates accurate to within 5-10 meters, precise timestamps, device information, and camera settings. This data is easily extractable using free tools like ExifTool.

A 2019 study published in the International Journal of Information Security found that 70% of smartphone users were unaware that photos contained GPS coordinates, and 89% didn't know how to remove this data. This represents a massive, largely unrecognized privacy vulnerability.

Metadata Removal

The EFF recommends making metadata removal an automatic habit before sharing any photo. On iOS, the share sheet includes an Options menu with a Location toggle. More reliably, apps like Metapho (available free on the App Store) strip all metadata before sharing. On Android, Photo Metadata Remover and Scrambled Exif provide similar functionality.

Prevention is preferable to remediation. On iOS: Settings > Privacy & Security > Location Services > Camera > Never. On Android: Camera app > Settings > disable "Location tags". Future photos won't contain GPS data.

Visual Analysis

Even without GPS metadata, photos reveal location through visual content. The EFF's protest guide (applicable to anyone concerned with identification or location) emphasizes examining photos for house numbers, street signs, business names, distinctive landmarks, license plates, school identifiers, visible mail or packages, and reflections in windows or mirrors.

Research from Carnegie Mellon University demonstrated that trained analysts could identify locations from photos with no metadata by analyzing architectural features, vegetation, street furniture, and other visual markers. Before posting any photo, zoom in on backgrounds and corners. If location is identifiable, crop it out, blur it, or don't share it.

Secure Communications

The EFF has extensively researched messaging security through their Secure Messaging Scorecard project. The findings are stark: standard SMS messages are fundamentally insecure, not encrypted, and accessible to phone carriers, law enforcement, and potential interceptors.

Signal: The EFF Recommendation

The EFF calls Signal "the gold standard for secure messaging." Signal is free, open-source, and provides end-to-end encryption, meaning even Signal cannot read messages. Unlike platforms owned by advertising-driven companies, Signal collects minimal metadata. The app is funded by grants and donations from the Signal Foundation, not user data monetization.

For sensitive conversations about safety, location, meetings, or anything requiring confidentiality, the EFF unequivocally recommends Signal.

Comparative Security

WhatsApp provides end-to-end encryption but is owned by Meta (Facebook), whose business model centers on data collection. As the EFF notes, "WhatsApp's encryption is strong, but Meta's business model is surveillance." While message content is protected, extensive metadata about communication patterns is collected.

iMessage encrypts conversations between Apple users but falls back to unencrypted SMS when messaging Android users. Many users don't understand this distinction. Additionally, messages stored in iCloud backup are accessible to Apple.

Facebook Messenger offers "Secret Conversations" with encryption but requires manual activation for each conversation. Standard messages are unencrypted and processed for advertising purposes.

Security Practices

Beyond app selection, the EFF recommends specific practices. Enable disappearing messages in Signal (Settings > Privacy > Default timer) so conversations auto-delete after a set period. Disable message previews on lock screens (iOS: Settings > Notifications > Messages > Show Previews > Never; Android: Settings > Notifications > Hide sensitive content).

Verify Signal safety numbers for important contacts. This cryptographic verification ensures you're communicating with the intended recipient and not an impersonator.

Certain information should never be transmitted digitally, even via encrypted messaging: complete passwords, full credit card numbers, Social Security Numbers, both sides of identification documents, physical security codes, or the most sensitive safety information. Digital data can be screenshotted, forwarded, subpoenaed, or recovered after deletion.

Data Brokers and Public Records

Data brokers collect personal information from public records, online activity, purchase histories, and other brokers, then sell it commercially. The EFF's 2023 analysis stated bluntly: "The data broker industry operates in the shadows, amassing detailed dossiers on hundreds of millions of people without their knowledge or consent."

Industry Scope

A 2014 Federal Trade Commission report on data brokers found that the industry maintains information on nearly every U.S. consumer, often including sensitive data like financial information, purchase behavior, and even health conditions. More recent research from Duke University's Sanford School of Public Policy estimated that the top data brokers maintain files on over 700 million consumers globally.

These companies provide easy access to current and past addresses, phone numbers, ages, relatives' names, email addresses, property ownership, court records, and more. Some offer basic information free; others charge small fees.

Opt-Out Process

The EFF acknowledges that opting out is "an endless game of whack-a-mole." Data reappears as databases are refreshed. New brokers emerge. But temporary removal still creates friction, making you harder to find through casual searches.

Major data broker sites—Spokeo, Whitepages, BeenVerified, Intelius, PeopleFinder, TruthFinder, Instant Checkmate, and MyLife—all maintain opt-out procedures. Each requires searching for your listing, then following site-specific opt-out processes involving form submission and email verification.

This process requires several hours initially and should be repeated quarterly. For high-risk individuals who can afford it, services like DeleteMe (approximately $129 annually) or Privacy Bee (approximately $197 annually) automate opt-out submissions across dozens of sites.

Digital Footprint Monitoring

Set up Google Alerts for your name to receive notifications when it appears online. Conduct monthly searches for your name plus your city. Check Google Images, not just text results. Try name variations and old addresses.

A 2021 Pew Research Center survey found that 79% of Americans are concerned about how companies use their data, yet only 20% say they regularly check their online presence. Regular monitoring allows rapid response to new exposures.

Email and Account Security

The EFF has long emphasized that standard email "was not designed with privacy in mind" and most email is "as private as a postcard." Email travels unencrypted across the internet unless both sender and recipient use encrypted email services.

Email Compartmentalization

The EFF recommends maintaining separate email addresses for different purposes: personal/private for family and banking, professional for work, and disposable for online shopping and subscriptions. If one account is compromised, others remain isolated.

Encrypted Email

ProtonMail and Tutanota both offer free encrypted email services. ProtonMail is based in Switzerland, which has strong privacy laws, and has been praised by the EFF for its privacy architecture. Tutanota is based in Germany and is fully open-source.

Two-Factor Authentication

The EFF's guide on two-factor authentication identifies it as one of the most important security measures available. Two-factor authentication requires both a password and a second verification method (typically a code from an authenticator app or sent via text) to access an account.

According to Google's 2019 security research, enabling two-factor authentication blocks 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks. It should be enabled on all email accounts, banking and financial services, social media, cloud storage, and any account containing sensitive information.

Authenticator apps (Google Authenticator, Authy, Duo Mobile) are more secure than SMS-based verification because SMS can be intercepted through SIM-swapping attacks.

Physical Privacy Protections

Address Confidentiality Programs

Many states operate address confidentiality programs for victims of domestic violence, stalking, sexual assault, or human trafficking. These programs provide a substitute address managed by the state, with mail forwarded to the participant's actual address. The National Network to End Domestic Violence maintains a directory of state programs.

Participants can use the substitute address on driver's licenses, voter registration, court documents, and other official records. Application typically requires assistance from a victim services advocate.

Alternative Addresses

The EFF recommends minimizing use of home addresses wherever possible. Commercial mail receiving agencies (CMRAs) like UPS Stores provide alternative addresses for $10-30 monthly. Use these for online shopping, subscriptions, business registrations, and any non-official correspondence.

Vehicle Privacy

Automated License Plate Readers (ALPRs) are deployed across the United States, photographing license plates and storing the data. The EFF's research on ALPRs found that billions of license plate scans are retained in databases accessible to law enforcement and private companies.

Never post photos showing license plates. Request Google Maps blurring if your vehicle appears in Street View imagery with visible plates (available at google.com/maps through the "Report a problem" feature). Park in garages when possible, back into parking spaces to reduce plate visibility, and avoid repeatedly parking in the same public location.

Credit Protection

Credit freezes prevent anyone, including you, from opening new credit accounts in your name. They're free and recommended by consumer protection organizations for at-risk individuals. Contact all three credit bureaus: Experian, TransUnion, and Equifax through their respective websites.

You'll receive a PIN to temporarily "thaw" the freeze when applying for legitimate credit. According to the Federal Trade Commission, credit freezes are the most effective protection against identity theft.

Building Sustainable Privacy Practices

The EFF's Surveillance Self-Defense project emphasizes that privacy requires ongoing attention, not one-time action. Technology changes, platforms update privacy settings without clear notification, and personal circumstances evolve.

Sustainable privacy practices involve daily habits: reviewing app location permissions, thinking before posting, removing photo metadata, using Signal for sensitive conversations, and locking devices. Weekly reviews should cover checking social media tags, auditing app permissions, and reviewing financial accounts. Monthly maintenance includes self-searches, privacy setting reviews, and password updates. Quarterly deep-dives involve data broker opt-out resubmissions,

comprehensive digital footprint searches, and credit report checks. Annual audits should include full password updates, account purges, document shredding, and physical security reviews.

Research from the University of Michigan School of Information found that users who maintained regular privacy check-ins discovered and remediated significantly more privacy issues than those who addressed privacy only reactively.

Conclusion

Privacy in the digital age requires active effort. The surveillance infrastructure built into modern technology won't disappear. Data brokers won't voluntarily stop collecting information. Social media companies won't abandon advertising-driven business models. Law enforcement capabilities will continue expanding.

But as the Electronic Frontier Foundation has demonstrated through decades of advocacy and technical guidance, individuals can reclaim meaningful privacy through informed action. The steps outlined here—disabling location tracking, configuring social media privacy settings, removing photo metadata, using encrypted messaging, opting out of data brokers, and building sustainable practices—create real barriers to surveillance and harassment.

Start with fundamentals: disable phone location services, set social media to private, install Signal, remove photo metadata, and search for yourself online. These five actions, implementable within an hour, establish a foundation. Build from there incrementally.

For someone facing stalking, harassment, or domestic violence, these steps can be lifesaving. For anyone concerned about privacy, they're essential. The right to privacy, as the EFF maintains, is the right to be yourself without surveillance.

Resources and Further Information

Primary Privacy Organizations

Electronic Frontier Foundation
The leading nonprofit defending digital privacy and civil liberties
Main site: https://www.eff.org/
Surveillance Self-Defense Guide: https://ssd.eff.org/

Privacy Rights Clearinghouse
Comprehensive privacy resources and consumer guides
https://privacyrights.org/

National Network to End Domestic Violence - Safety Net Project
Technology safety resources for abuse survivors
https://www.nnedv.org/safetynet
https://www.techsafety.org/

Coalition Against Stalkerware
Information about phone monitoring software and protection
https://stopstalkerware.org/

Emergency Resources

National Domestic Violence Hotline
24/7 confidential support
Phone: 1-800-799-7233
https://www.thehotline.org/

RAINN (Rape, Abuse & Incest National Network)
National Sexual Assault Hotline
Phone: 1-800-656-4673
https://www.rainn.org/

National Center for Victims of Crime
Resources and advocacy
https://victimsofcrime.org/

Stalking Resource Center
Information and support for stalking victims
https://victimsofcrime.org/our-programs/stalking-resource-center/

Privacy Tools

Signal
EFF-recommended secure messaging
https://signal.org/

ProtonMail
Encrypted email service
https://proton.me/mail

Tutanota
Open-source encrypted email
https://tutanota.com/

Privacy Badger
EFF-created browser extension blocking trackers
https://privacybadger.org/

ExifTool
Photo metadata removal tool
https://exiftool.org/

Bitwarden
Open-source password manager
https://bitwarden.com/

Metapho (iOS)
Photo metadata viewer and remover
https://apps.apple.com/us/app/metapho/id914457352

Data Broker Opt-Out Resources

Privacy Rights Clearinghouse Data Broker Database
Comprehensive list with opt-out instructions
https://privacyrights.org/data-brokers

DeleteMe
Paid service for automated opt-outs
https://joindeleteme.com/

Privacy Bee
Automated data removal service
https://privacybee.com/

Government and Legal Resources

Federal Trade Commission - Identity Theft and Online Security
https://consumer.ftc.gov/features/identity-theft-and-online-security

Federal Trade Commission - Credit Freezes
https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts

National Network to End Domestic Violence - Address Confidentiality Programs
State-by-state directory
https://www.nnedv.org/content/address-confidentiality-programs/

Credit Bureau Security Freezes

Experian
https://www.experian.com/freeze/center.html

TransUnion
https://www.transunion.com/credit-freeze

Equifax
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Educational Resources

Consumer Reports Security Planner
Personalized privacy and security recommendations
https://securityplanner.consumerreports.org/

Krebs on Security
Cybersecurity news and practical advice
https://krebsonsecurity.com/

Google Alerts
Monitor when your name appears online
https://www.google.com/alerts

Google Maps - Report a Problem
Request blurring of images
https://support.google.com/maps/answer/7011973

Academic and Research Resources

Pew Research Center - Privacy and Data
Research on Americans' privacy attitudes and behaviors
https://www.pewresearch.org/topic/internet-technology/privacy-data/

Surveillance Self-Defense - EFF Module Index
Comprehensive privacy guides for different scenarios
https://ssd.eff.org/module-categories/tool-guides

Platform-Specific Privacy Settings

Apple Privacy Guide
https://support.apple.com/guide/iphone/welcome/ios (Privacy section)

Google Privacy & Security Settings
https://myaccount.google.com/security

Facebook Privacy Settings
https://www.facebook.com/privacy/

Instagram Privacy Settings
https://help.instagram.com/196883487377501

Note: This guide is for educational purposes only. For legal advice specific to your situation, consult a licensed attorney. For immediate safety concerns, contact emergency services (911) and victim advocacy organizations.

Last Updated: January 1, 2026