

Foundations: Data, Privacy & Surveillance

Understanding the digital trail, access methods, and protective measures.

Personal data is a digital trail of your life

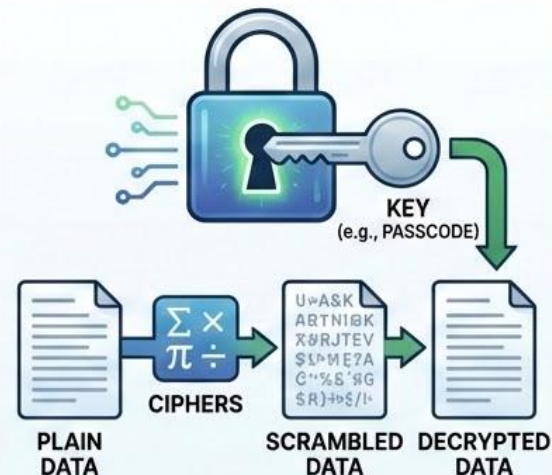


How Data is Accessed



Data is collected through legal warrants, purchased from data brokers, or intercepted via tracking technology.

Encryption

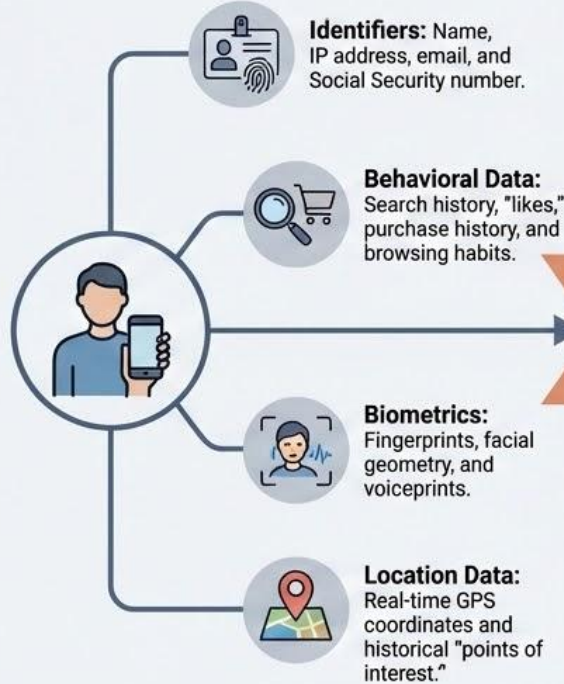


This is your primary defense. It uses mathematical "ciphers" to scramble your data so that only someone with the correct "key" (like your passcode) can read it.

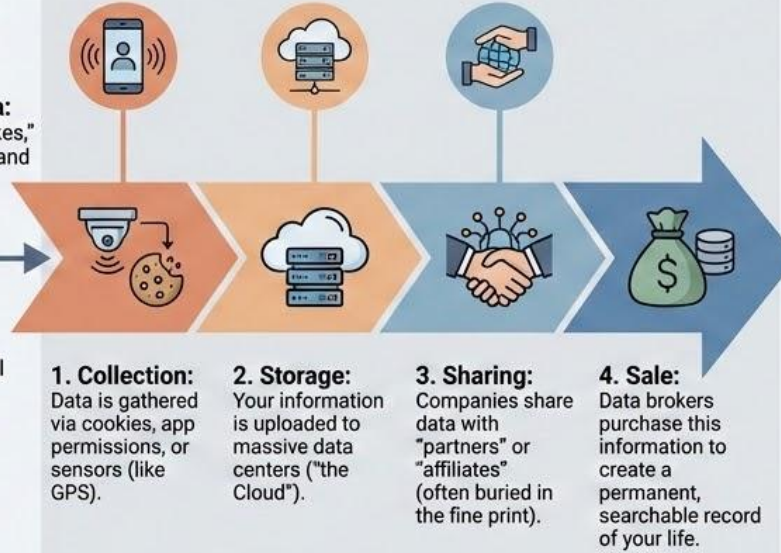
Digital Surveillance: A Foundation for Understanding & Protection

Digital surveillance is the automated collection, analysis, and storage of your digital life. Every interaction with a smartphone, app, or website leaves a trail that can be reconstructed to map your habits, relationships, and beliefs.

Your Digital Footprint (Personal Data)



The Data Flow Pipeline



The Watchers & Their Motives



Government Surveillance

Motive: Law enforcement and national security.

Methods: It involves tools like warrants for phone records or "Stingrays" to track protesters.



Corporate Tracking

Motive: Driven by profit. Companies track you to build "user profiles" that keep you engaged with their platforms and show you targeted advertisements.

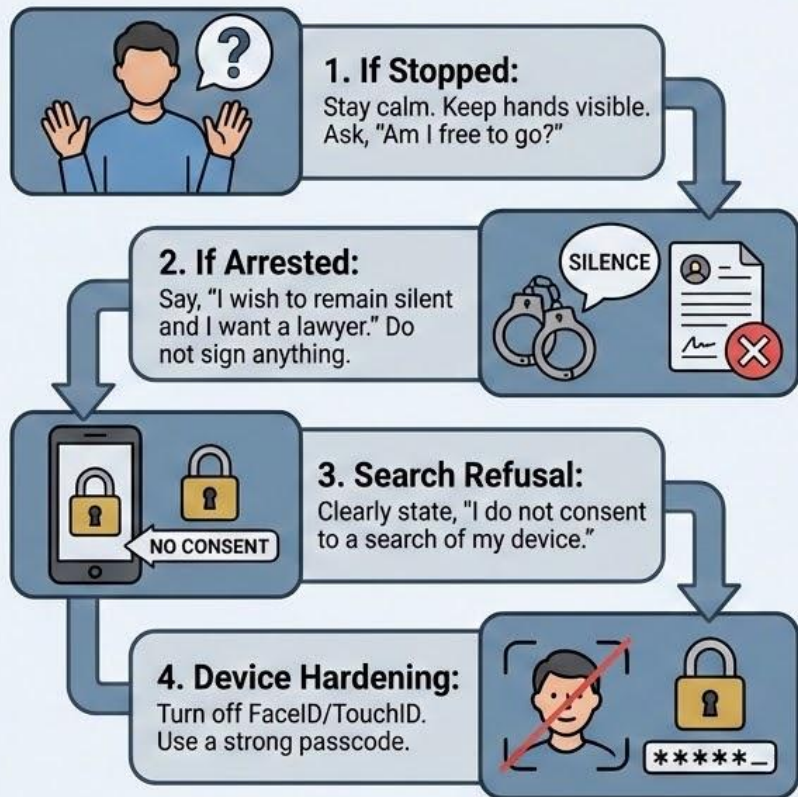


Data Brokers

Motive: These companies act as "middlemen." They collect data from public records and private apps, bundle it, and sell it to anyone—from advertisers to government agencies.

KNOW YOUR DIGITAL RIGHTS: IMMEDIATE ACTIONS & LEGAL PROTECTIONS

IMMEDIATE ACTIONS (REACTIVE STEPS)



YOUR LEGAL RIGHTS (FOUNDATIONAL PRINCIPLES)



YOUR LEGAL RIGHTS: DIGITAL PRIVACY & CONSTITUTIONAL PROTECTIONS



THE FOURTH AMENDMENT

FUNDAMENTAL SAFEGUARDS: Rooted in the U.S. Constitution and NY State Constitution, providing immunity against “unreasonable searches and seizures”.

- **SECURING CITIZENS:** Protects against arbitrary government intrusion.
- **LEGAL STANDARDS:** Permits limited stop-and-frisk based on an officer's “reasonable suspicion” of criminal activity.
- **NY STATE PROTECTIONS:** Article I, § 12 offers more expansive liberty and privacy protections than federal law.
- **REASONABLENESS SCRUTINY:** NY courts mandate police encounters be scrutinized for reasonableness from inception, not just at forcible stop.



Reasonable Suspicion
vs.
Arbitrary Intrusion.

THE FIFTH AMENDMENT

PROTECTING YOUR MIND: While the Fourth Amendment protects your device, the Fifth Amendment protects your testimonial privilege.

- **TESTIMONIAL PRIVILEGE:** Courts generally agree that providing a password or encryption key is “testimonial”.
- **YOUR RIGHT:** You cannot be forced or threatened into giving up your password or unlocking your device to self-incriminate.
- **BIOMETRIC RISKS:** Using biometric authentication (facial/fingerprint scan) may **compromise** the privilege against **compelled** self-incrimination regarding device contents.



LIMITS ON POLICE ACCESS TO PHONES, LAPTOPS, AND CLOUD ACCOUNTS

Even if you're arrested, police can only search your phone under limited circumstances.

PHYSICAL ITEMS (ON PERSON / IMMEDIATE CONTROL)



After a person has been arrested, the police generally may search the items on her person and in her pockets, as well as anything within her immediate control, automatically and without a warrant.



**AUTOMATIC SEARCH ALLOWED
(NO WARRANT)**

DIGITAL DATA (PHONES, LAPTOPS, CLOUD)



But the Supreme Court has ruled that police cannot search the data on a cell phone warrant.



**SEARCH RESTRICTED
(WARRANT REQUIRED)**



SUPREME COURT RULING APPLIES

Note: This is a general overview. Legal specifics can vary. Consult a lawyer for advice.

Exceptions to the Warrant Requirement (Searches Without a Warrant)

Primary legal contexts where authorities do not need a warrant to search your person/data:

Informed Consent



Voluntarily consenting to be searched, providing an officer with your passcode or permission to inspect your device constitutes a waiver of your Fourth Amendment protections. You can limit the scope of that consent and even revoke or take it back after the officers begin searching. You maintain the legal right to state, "I do not consent to a search."

Border and Port-of-Entry Searches



Federal authorities at international boundaries and airports are authorized to inspect electronic devices without a warrant, even if they have no reason to suspect there is anything illegal on it.

The "100-Mile Border Zone" establishes a broad geographic area where federal agents are granted enhanced powers, allowing "reasonable" stops and searches even without probable cause or a warrant. In the border zone, privacy interests are frequently subordinated to national security imperatives.

WARRANT REQUIREMENT (Fourth Amendment)

The Third-Party Doctrine



Police can ask your roommate/guest/spouse/partner to search the premises or for access to your computer if they don't have a warrant.

Information that is voluntarily disclosed to third parties, including your ISP, mobile carrier, or public social media platforms, may be subject to diminished privacy protections under current law.

Tip: Advise all members of your household to explicitly withhold consent for any searches requested by law enforcement.

Threat of Destruction of Evidence



If police have probable cause to believe there is incriminating evidence in the house or on an electronic device that is under immediate threat of destruction, they can immediately search it without a warrant.

Encounters with Law Enforcement at Home and at Protests



Your Rights if Police or ICE are at your home



Warrant Requirement & Entry:

Police need a warrant to enter. You do not have to let them in without one.

Authorities with an arrest warrant can enter *if* they have a reasonable belief the subject is inside.

Valid Warrant Checklist:

- ☒ Correct name/address
- ☒ List of items to be seized
- ☒ Judge's signature
- ☒ Deadline for execution

Administrative Warrant (I-205):



Does **NOT** grant authority to enter a residence without informed consent.

Your Digital Rights during a Police Encounter

With a Valid Warrant:



Seizure: Devices can be seized for forensic examination and media duplication.



Passwords & Encryption: Not legally compelled to provide keys/passwords. No coercion allowed. A judge may mandate decryption; seek legal counsel immediately.

Cloud Backups:



Law enforcement can obtain unencrypted backups from cloud providers (Apple, Google).

Mitigation Protocols: Stop cloud backups, enable Advanced Data Protection (iCloud), or use encrypted backups (e.g., WhatsApp).

Device State:



Unlocked Device: All encrypted messages become accessible.



Locked Device: MDFT Tools (Cellebrite, GrayKey) can bypass security. Agencies may use remote spyware for access.



Your Rights Online: Employer Surveillance

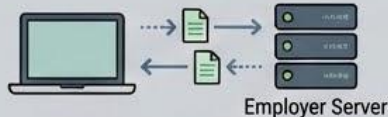
PRIVATE SECTOR EMPLOYERS



Surveillance Tools & Methods

-  closed-circuit video monitoring
-  internet monitoring and filtering
-  email monitoring
-  instant message monitoring
-  automatic time tracking
-  phone monitoring
-  location monitoring
-  personality and psychological testing
-  keystroke logging

Data Collection & Privacy Invasion



Some programs send employees' location information, screenshots of their devices, or emails directly to the employer.



Some services allow employers to remotely activate employees' webcams and microphones without their knowledge.

This surveillance subjects employees to serious privacy invasions, and employees have little to no choice as to whether they are surveilled if they want to continue their employment.

PUBLIC SECTOR EMPLOYEES



Public Sector Employees cannot be placed under persistent electronic surveillance or be fired for their beliefs or criticisms of the government unless it impacts their ability to serve the public.



You have some Fourth Amendment protection in your office or workspace. This means the police need a warrant to search your office and work computer unless you (or your employer) consent or there is probable cause.



But the extent of Fourth Amendment protection depends on the physical details of your work environment, as well as any employer policies.



Your employer can consent to a police request to search an office or workspace in your absence.



If you work for a public entity or government agency, no warrant is required to search your computer or office as long as the search is for a non-investigative, work-related matter.

Rights During Police Encounters: Protecting Your Devices and Digital Data



Police Authority & Warrants

- With a warrant, police can seize the computer/device and take it for a thorough search.
- As part of the inspection, police may make a copy of media or other stored files.
- If your computer was illegally taken, you can file a motion with the court to have it returned.
- Police can keep the computer as evidence if they believe it contains evidence of a crime (e.g., digital contraband).
- Police may attempt permanent forfeiture, which you can challenge in court.



Your Rights (5th Amendment)

- The Fifth Amendment protects you from being forced to give self-incriminating testimony (like passwords or encryption keys).
- A police officer cannot force or threaten you into giving up your password or unlocking your devices.
- Biometrics (face scan, fingerprint) may compromise 5th Amendment protections against compelled incrimination.
- Using a memorized passcode generally provides a stronger legal footing to push back against a court order.
- A judge or grand jury may be able to force decryption in some circumstances. Seek legal help.



Threats & Vulnerabilities

- If someone has physical access to your unlocked phone (e.g., during an arrest), they can read all encrypted messages.
- Even if locked, police have tools (Cellebrite, Greykey) to try to unlock phones and read encrypted messages.
- If physical access fails, police could try to remotely plant spyware, giving them full access to everything, including encrypted messages.



Proactive Data Protection

- Law enforcement can get a backup of your text messages from your cloud provider (Apple, Google) as they are often stored unencrypted by default.
- **TIP:** Either "do not use backups, enable Advanced Data Protection for iCloud if you have an iPhone, or enable encrypted backups in apps like WhatsApp if you are worried about the government reading your messages."

YOUR DIGITAL RIGHTS DURING PROTESTS: ANONYMITY, RECORDING, & DATA PROTECTION



ANONYMITY & IDENTIFICATION PROTOCOLS

-  Use **face coverings** to avoid facial recognition surveillance.
-  Activate **"Airplane Mode"** or **power down** to stop real-time tracking.
-  **Deactivate facial & fingerprint recognition**; use a strong passcode.
-  **Ride a bike** or **walk** to avoid Automated License Plate Readers (ALPR).
-  Consider a **prepaid, disposable phone**. Fully **encrypt** device data & use encrypted messaging apps (Signal, WhatsApp).



RECORDING POLICE



-  You have a **First Amendment right** to record police performing duties in public.
-  Police **cannot delete** your photos or videos.
-  Police **need a warrant** to search your device or view contents, even if arrested.
-  Right to **photograph in public spaces**; private property owners set rules.



INTERFERENCE EXCEPTION: Law enforcement may order cessation if truly interfering with legitimate operations.



METADATA & POST-PROTEST ACTIONS

-  Photos contain **metadata** (GPS, timestamps, device info).
-  **Scrub metadata** to prevent tracking of location, time, and identity.
-  **Transfer photo to computer**, take a **screenshot**, and **post** the screenshot, not the original.
-  **Exercise caution: blur faces and identifiers** before posting; avoid live-streaming faces.

Securing Your Communications: Encrypted Messaging

The Vulnerability of SMS



The Vulnerability of SMS

Standard SMS/MMS: Not usually encrypted. Phone companies store copies often requested by law enforcement.

Network Risks: Agencies like the NSA can capture messages over the network using technologies like cell-site simulators.

~ When a message is not encrypted, your phone company can and will often store a copy.

Signal: The Gold Standard



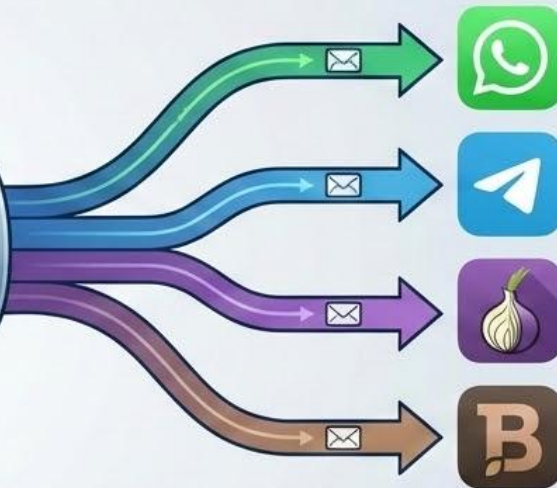
Signal: The Gold Standard

End-to-End Encryption: Only sender and receiver can read content. Signal cannot access messages.

Minimal Metadata: Intentionally stores only what's required for operation, protecting against data brokers and court orders.

- Disappearing messages
- Username (no phone number)
- Hide message previews
- Safety numbers for verification.

Secure Alternatives



Secure Alternatives

Session: Best for anonymous texting without phone numbers.

WhatsApp: Biggest user base, though metadata policies differ.

Briar: Designed for avoiding surveillance in high-risk areas.

Telegram: Strong social networking features.

Source: Kim Key, PCMag (2025).

Private Browsing vs. VPNs: Understanding the Differences



PRIVATE BROWSING (INCOGNITO MODE)



WHAT IT DOES:

- Erases browsing & search histories
- Deletes cookies & site data on exit
- Clears form data & logins
- Good for public/shared computers



WHAT IT DOESN'T DO:

- Hide activity from ISP, employer, or school
- Prevent tracking by routers, firewalls, & proxies
- Delete downloaded files or new bookmarks
- Protect against malware or phishing



VIRTUAL PRIVATE NETWORKS (VPNs)



WHAT IT DOES:

- Encrypts internet traffic
- Masks your actual IP address
- Changes virtual location (geo-spoofing)
- Bypasses censorship & accesses restricted content
- Secure remote access to corporate networks



WHAT IT DOESN'T DO:

- Make you completely anonymous (VPN provider sees traffic)
- Block ads or cross-site trackers
- Delete local browser history or cookies
- Protect from law enforcement requests to VPN provider

KEY TAKEAWAY: Incognito mode handles local privacy on your device, while a VPN secures your connection and masks your location online. For comprehensive privacy, they are often used together.

LOCATION SHARING: LIKE BEING FOLLOWED AROUND 24/7



Both cellular service providers and apps collect records of cell phone locations. via cell-tower records or "geo-fence". Long-term tracking requires a warrant; short-term may not.

MOBILE SIGNAL TRACKING TOWERS



Triangulation calculates phone location when powered on and registered. No way to hide if phone is on. Government can force operator to turn over location data. "Tower dump" provides list of devices in an area at a time (e.g., crime, protest).

CELL SITE SIMULATOR (IMSI CATCHER)



Portable fake cell phone tower collects location data directly. Must be physically nearby. Detects physical presence. Currently no reliable defense.

WI-FI AND BLUETOOTH TRACKING



Device's unique MAC address observed in wireless signals, even if not connected or active. Wi-Fi transmits occasional signals with MAC address. Short range (room/building).

LOCATION LEAKS FROM APPS AND WEB BROWSING



Smartphones determine location via GPS, Wi-Fi, cell towers. Apps transmit location to service provider, allowing others to track you.

Note: This is a general overview. Legal specifics can vary.

Practical Self-Protection & Device Security

SECURE YOUR HARDWARE



Prioritize Passcodes over Biometrics



Law enforcement can legally compel biometrics.

Passcodes have stronger Fifth Amendment protection.

Action: Disable FaceID/TouchID in high-risk situations; use strong, unique alphanumeric passcode.



Enable Full-Disk Encryption



Ensure device is encrypted so data remains scrambled if seized. Mostly enabled by default.

AUDIT APP PERMISSIONS



Manage Access & Data



Location: Set to "Only While Using" or "Never" (not "Always On").



Privacy Settings: Limit post visibility and personal info.



Ad Tracking: Disable to reduce targeted ads.



VPN: Use to hide IP address.



Incognito Mode: Hides local history, not from websites/ISP.



Mic/Camera: Disable access; turn on only when needed.

BIOMETRIC DATA & FACIAL RECOGNITION



Pros & Cons



Why use a Biometric ID? (Convenience & Security)

Faster than typing; harder to steal/guess; can combine with PINs (MFA) for apps/payments.



Privacy Concerns (Risks & Limitations)

Not 100% secure (can be tricked); Cannot be changed if compromised; Data storage risks if locally breached.

DEPLOYING END-TO-END ENCRYPTION



Secure Messaging Protocols



SMS/MMS/RCS lack encryption, accessible to providers and law enforcement.



Signal Messenger (Recommended)

Prioritizes minimal data, open code. **End-to-End Encryption (E2EE):** Only sender/receiver can read messages.



Integrated Protections:

Disappearing Messages; Pseudonymous Usernames; Suppressed Previews; Privacy Settings (hide phone number); Safety Numbers.

Alternative Encrypted Platforms



Session (High-anonymity);



WhatsApp (Expansive base);



Briar (Avoid surveillance);



Telegram (Social networking).

Actions to Take if Your Rights are Violated

Procedures for Documenting an Incident



- ✓ **Detailing the Encounter:** Record every available detail while fresh, including officer badge numbers, patrol vehicle identifiers, the specific agency, and a full narrative of events.
- ✓ **Witness Coordination:** Secure names and contact information for any individuals who observed the police interaction.
- ✓ **Physical Evidence:** Should injuries occur, prioritize immediate medical care and document all physical trauma through comprehensive photography.
- ✓ **Formal Complaints:** File a written grievance with the agency's internal affairs division or a civilian complaint board; anonymous submissions are typically permitted.

Requesting Records: FOIA & State Equivalents



- ✓ **Accessing Federal Files:** To retrieve documentation regarding your interactions with Border Patrol, submit a Freedom of Information Act (FOIA) or Privacy Act request via the DHS FOIA website.
- ✓ **Reporting CBP Misconduct:** Formal grievances specifically concerning Customs and Border Protection should be filed through the CBP INFO Center at help.cbp.gov.

How to Challenge Unlawful Search and Seizure



- ✓ You retain the right to file a motion with the court demanding its return.
- ✓ If law enforcement determines that the computer contains evidence of a crime, such as digital contraband or illicit imagery, the device may be retained as evidence.
- ✓ Authorities may pursue permanent retention through a legal process termed forfeiture, which must be challenged via judicial proceedings.

Legal Resources & Advocacy Organizations



- ✓ **Access Now:** Offers a specialized Digital Security Helpline provided in nine languages.
- ✓ **ACLU:** Provides a comprehensive Guide for Immigrants' Rights for legal navigation.
- ✓ **National Immigration Law Center:** Maintains an updated Guide to Your Rights for protective measures.
- ✓ **Local Assistance:** Access the Find Help For Immigrants Near You directory for NYC-based community organizations.

Protecting Your Rights: Documentation & Legal Redress



1. Document Incidents

- **Detailed Records:** Write down Badge #s, car IDs, agency
- **Witnesses:** Secure contact info from observers
- **Medical:** Seek care & photograph injuries
- **Complaints:** File with internal affairs



2. Records & Reporting

Border Patrol Records:

Submit FOIA request:
dhs.gov/foia-request

Reporting CBP Abuses:

CBP INFO Center: help.cbp.gov



3. Help & Guidance

Access Now: Digital Helpline
accessnow.org/help

ACLU: Immigrants' Guide
aclu.org/know-your-rights

National Immigration Law Center:
Rights Guide
media.nilc.org

Informed Immigrant:
informedimmigrant.com

Tracking Your Online Activity

Companies track your online activity by:



Saving your preferences and information;



Showing you personalized content;



Gathering analytics about your visit to a website;



Remembering the things you searched for online.

How they work: Cookies, Trackers, and Targeted Media

Collect

Data Collection & First-Party vs. Third-Party Tracking



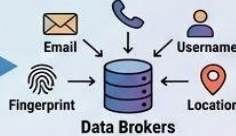
Online trackers collect millions of data points about us each day.

First-party tracking allows a website you visit to track you.

Third-party tracking lets another company track you across websites you visit.

Link

Linking Data & Building Profiles



Pieces of personal data about us are linked through established logins or known credentials and used to track, profile, or target us across the online ecosystem.

Web browsers use small files called "cookies" to store information about your interactions with sites. Even if blocked, information about the consumer's computer configuration can be used as a sort of "fingerprint" to link their data.

Profile

Targeting & Personalized Ads



This aggregated personal data is then used to create intimate profiles about us in order to target us with "personalized" advertisements that stalk us across the web.

Devices tracking your data include:



Phones, laptops, tablets, and gaming devices



Cameras, doorbells, and security systems



"Smart" devices like smart watches, smart TVs, and smart speakers collect personal data even when people are not interacting with them



Internet, cable, and phone companies

Apps often collect more data than websites:



Social media apps



Messaging apps



Health apps



Mapping, rideshare, and delivery apps



Banking, budgeting, and stock-trading apps



Dating apps and Shopping apps

Digital Defense: A Guide to Your Rights & Privacy in the Surveillance Age

FOUNDATIONS OF THE DIGITAL TRAIL



PERSONAL DATA IS YOUR DIGITAL BIOGRAPHY

Includes identifiers (IP addresses), behavioral data (search history), biometrics (face geometry), and location data (GPS coordinates).

THE THREE FACES OF SURVEILLANCE



Government
(National Security)



Corporations
(Profit-Driven Profiles)



Data Brokers
(Bundle & Sell Life History)

HOW YOUR DATA FLOWS



COLLECTION
(Sensors/Cookies)



STORAGE
(The Cloud)



SHARING
(Partners)



SALE
(To Brokers)

TECHNICAL DEFENSIVE TOOLS



END-TO-END ENCRYPTION (E2EE)

Ensures only sender and receiver can read a message; provider cannot access content.



SIGNAL: THE PRIVACY STANDARD

Nonprofit app, minimal metadata, disappearing messages, safety numbers, pseudonymous usernames.



VPN VS. INCOGNITO MODE

Incognito only hides history on device: VPN encrypts traffic and hides IP from ISP/websites.

CONSTITUTIONAL SHIELDS (4TH & 5TH AMENDMENTS)



4TH AMENDMENT: PROTECTING YOUR DEVICES

Safeguards against "unreasonable searches and seizures". New York state law (Art. 1 § 12) provides even broader protection.



5TH AMENDMENT: PROTECTING YOUR MIND

Protects against self-incrimination; courts generally agree a memorized passcode is "testimonial" and cannot be forced.



PASSCODES VS. BIOMETRICS

Alphanumeric passcodes offer stronger legal footing than biometrics (fingerprints/face scans), which can be legally compelled.

THE WARRANT GUARDRAIL & ITS EXCEPTIONS



THE PROBABLE CAUSE STANDARD

Warrants require substantiated belief of a crime and must specify exact location, person, and items.



THE THIRD-PARTY DOCTRINE

Information voluntarily shared with third parties (ISPs, banks, social media) has diminished privacy.



THE 100-MILE BORDER ZONE

Within 100 miles of U.S. border, federal agents have expanded powers for "reasonable" searches without warrants.

PROTOCOL FOR LAW ENFORCEMENT ENCOUNTERS



RIGHTS DURING PROTESTS

Right to record police; officers cannot delete data; use "Airplane Mode" to limit location tracking.



IF POLICE ARE AT YOUR DOOR

Do not let them in without judicial warrant; step outside, close door, verify document and judge's signature.



RECORDING AND METADATA

Scrub metadata (GPS/timestamps) from photos before posting by taking a screenshot and sharing that.

DATA TABLE: MOBILE SIGNAL TRACKING METHODS

METHOD	DESCRIPTION	DEFENSE
TOWER TRIANGULATION	Operators calculate position via cell towers.	Power down device entirely.
CELL SITE SIMULATOR	"Stingrays" mimic towers to catch nearby IDs.	No reliable defense; use E2EE.
WI-FI/BLUETOOTH	MAC addresses are broadcast even when not connected.	Turn off Wi-Fi and Bluetooth.
APP/GPS LEAKS	Apps transmit GPS data to service providers.	Revoke app location permissions.

References

- Albert M. Rosenblatt, *The Complete Search Warrant, Annotated*, N.Y. STATE UNIFIED CT. SYS., 37-38 (2004), https://www.nycourts.gov/judges/searchwarrant_manual.pdf (citing *People v. Bigelow*, 66 NY2d 417, 423 (1985)).
- AM. C.L. UNION, *IMMIGRANTS' RIGHTS*, <https://www.aclu.org/know-your-rights/immigrants-rights> (last updated Sept. 3, 2025).
- AM. C.L. UNION, *PROTESTERS' RIGHTS* (Jan. 30, 2026), <https://www.aclu.org/know-your-rights/protesters-rights>.
- AM. C.L. UNION OF DC, *HOW TO DEFEND AGAINST POLICE SURVEILLANCE AT PROTESTS*, (Jan. 10, 2017), <https://www.acludc.org/how-defend-against-police-surveillance-protests/>.
- BROOKLYN COLL. LIBR., *PHONE PRIVACY*, https://libguides.brooklyn.cuny.edu/digital_safety/phone (last visited Mar. 16, 2026).
- BROOKLYN COLL. LIBR., *SOCIAL MEDIA*, https://libguides.brooklyn.cuny.edu/digital_safety/social_media (last visited Mar. 16, 2026).
- COMM'N ON CIVIL RIGHTS, POLICE PRACTICES AND CIVIL RIGHTS IN NEW YORK CITY CH. 5 (2000), <https://www.usccr.gov/files/pubs/nypolice/ch5.htm>.
- Courtney Lindwall, *How to Use the Signal App for Secure Messaging*, CONSUMER REPORTS (Feb. 13, 2026), <https://www.consumerreports.org/electronics-computers/privacy/how-to-use-signal-app-secure-messaging-a4159663583/>.
- CTR. FOR DEMOCRACY & TECH., *TECH EXPLAINED: THE GLOSSARY*, (July 31, 2018), <https://cdt.org/insights/tech-explained-the-glossary/>.
- ELECTRONIC FRONTIER FOUND., *Can the Government Read My Text Messages?*, DIGITAL RIGHTS BYTES (Mar. 27, 2026), <https://www.digitalrightsbytes.org/topics/can-the-government-read-my-text-messages>.
- EPIC, ONLINE ADVERTISING & TRACKING, <https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/> (last visited Mar. 20, 2026).
- EPIC, *PRIVACY IN PUBLIC*, <https://epic.org/issues/surveillance-oversight/privacy-in-public/> (last visited Mar. 20, 2026).
- EPIC, *WORKER PRIVACY*, <https://epic.org/issues/data-protection/workplace-privacy/> (last visited Mar. 20, 2026).
- FED. TRADE COMM'N, *HOW WEBSITES AND APPS COLLECT AND USE YOUR INFORMATION* (Sept. 2023), <https://consumer.ftc.gov/articles/how-websites-apps-collect-use-your-information>.
- Hanni Fakhoury & Dia Kayyali, *Know Your Rights*, ELECTRONIC FRONTIER FOUND. (last updated Oct. 2014), <https://www.eff.org/issues/know-your-rights#4>.
- Ian Paul, *Three Practical Reasons to Use Your Browser's Private Mode*, PCWORLD (Mar. 11, 2014, 8:27 AM), <https://www.pcworld.com/article/444292/three-practical-reasons-to-use-your-browsers-private-mode.htm>.
- Joseph Jerome, *Techsplinations: Part 5, Virtual Private Networks*, CTR. FOR DEMOCRACY & TECH. (Oct. 16, 2018), <https://cdt.org/insights/techsplinations-part-5-virtual-private-networks/>.
- Kim Key, *The Best Private Messaging Apps for 2026*, PCMAG (Sept. 29, 2025), <https://www.pcmag.com/picks/best-secure-messaging-apps>.
- LEADERSHIP CONF. ON CIV. & HUM. RTS., *DIGITAL SECURITY BEST PRACTICES*, <https://civilrights.org/digital-security-best-practices/> (last visited Mar. 20, 2026).
- Lee Mathews, *What Is Private Browsing And Why Should You Use It?*, FORBES (Jan. 27, 2017, 1:00 PM), <https://www.forbes.com/sites/leemathews/2017/01/27/what-is-private-browsing-and-why-should-you-use-it/>.
- Maya Autorino, *Know Your Rights: Protecting Digital Privacy at the Border*, HUMAN RIGHTS FIRST (May 15, 2025), <https://humanrightsfirst.org/library/know-your-rights-protecting-digital-privacy-at-the-border/>.
- SURVEILLANCE SELF-DEFENSE, *THE PROBLEM WITH MOBILE PHONES*, ELECTRONIC FRONTIER FOUND. (Oct. 29, 2018), <https://ssd.eff.org/module/problem-mobile-phones>.
- U.S. CONST. amend. IV.
- U.S. SURVEILLANCE SELF-DEFENSE, *CHOOSING THE VPN THAT'S RIGHT FOR YOU*, ELECTRONIC FRONTIER FOUND. (Jan. 24, 2025), <https://ssd.eff.org/module/choosing-vpn-thats-right-you>.

This document offers guidance to help individuals protect their digital hygiene. But self-protection is not a panacea—lasting safety depends on stronger legal protections as well.

To learn more about the proposed New York Privacy Amendment and the policy landscape around digital privacy, contact Jared Trujillo at jared@equalityny.org.

