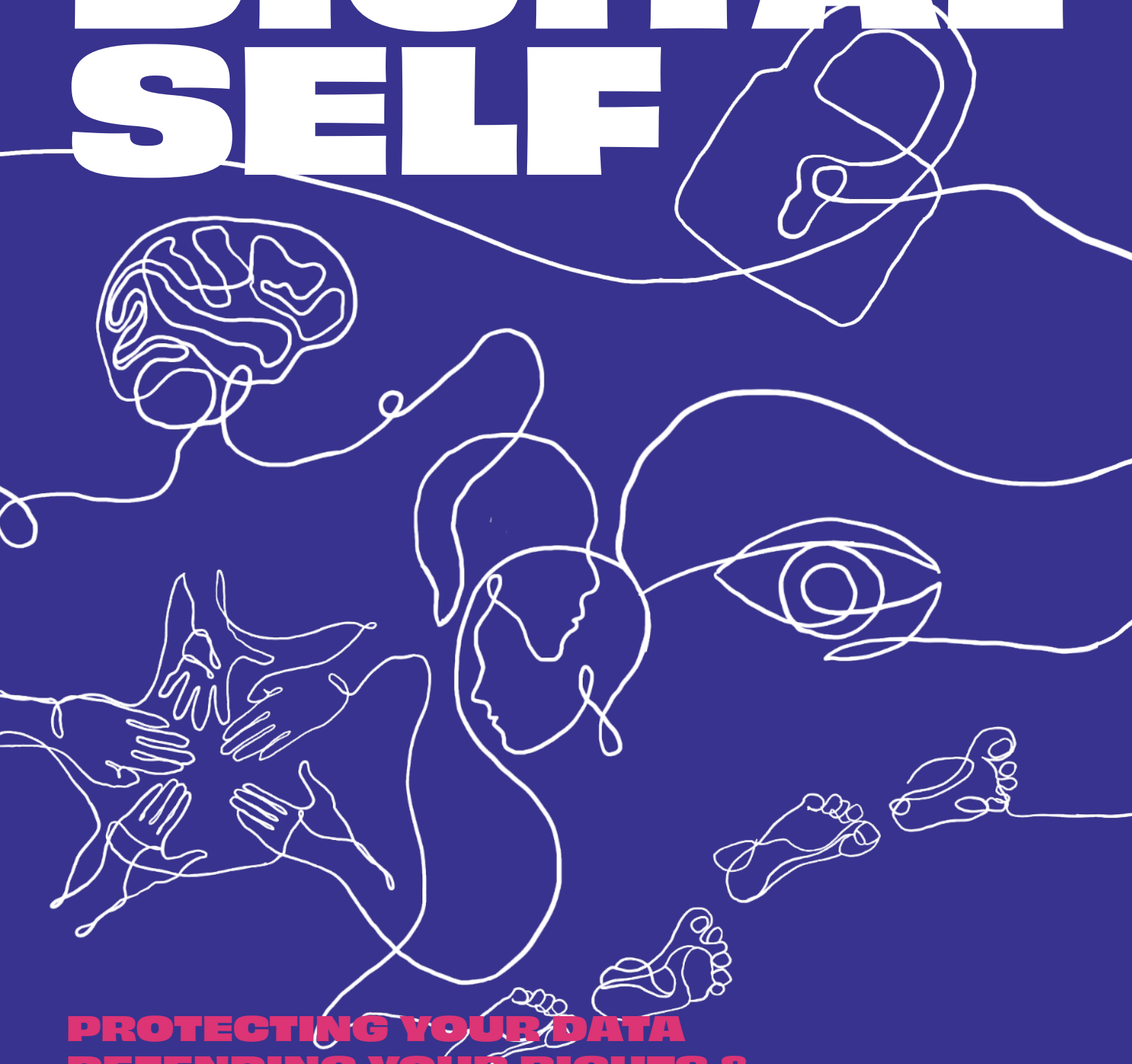
UNDERSTANDING YOUR DIGITAL SELF



**PROTECTING YOUR DATA
DEFENDING YOUR RIGHTS &
BUILDING BETTER FUTURES ONLINE.**

DEVELOPED & COORDINATED BY:

Avery Crower - Graduate Student at Parsons School of Design | MS Design and Urban Ecologies Program

ACKNOWLEDGMENTS:

Community Tech Lab NY - Luis Munive &
Oscar Comunidad

This toolkit is divided into 5 sections, each focused on a key system of your digital self. Use them together or individually, whatever best supports your needs.

Protect your digital self by keeping these 5 systems safe, strong, and secure.

DIGITAL

PREFACE

In today's world, navigating digital spaces is as important as navigating physical ones. Our devices, accounts, and online behaviors form an invisible extension of ourselves, which we call our digital self, or our digital body. Protecting this digital self is essential for preserving your privacy, autonomy, and safety.

This toolkit is a guide for anyone who wants to better understand how technology shapes their lives and how to take back some control.

HOW THIS TOOLKIT WORKS:

Your Digital Self is designed to be modular. Each section stands on its own, focusing on a different part of your digital self — starting with the core foundations of knowledge (Digital Literacy), to what you leave behind (Digital Footprint), to who's watching (Digital Surveillance), to how you appear online (Digital Presence), and how you can advocate for better systems (Digital Advocacy).

You can move through the toolkit in order or jump to the sections most relevant to you. Every topic offers practical tools, reflection exercises, and actionable steps to strengthen your digital health.

The toolkit uses the metaphor of a body scan, treating your digital self with the same care you give your physical self. Each section protects a different "vital system."

WHO IS THIS FOR:

This resource is for:

- Individuals who want to strengthen their digital privacy
- Community organizers and educators
- Youth groups, mutual aid networks, and advocacy organizations
- Anyone running workshops or conversations around digital rights, security, or inclusion

Whether you're just beginning your privacy journey or looking to sharpen your knowledge, this toolkit is made to be accessible and adaptable.

HOW TO USE IT:

Independently: Treat this toolkit like a guidebook. Choose a section to dive into, complete the reflection activities, and apply the practices to your everyday tech use.

In Shared Spaces: This toolkit is also workshop-friendly. Use the sections as modules for discussions, community trainings, or even casual group conversations. Reflection prompts, checklists, and activities are designed to be printable, shareable, and remixable.

In Workshops: Each section can be the foundation for a workshop session, classroom lesson, or community meeting. Start with a short discussion of the concepts, invite personal reflection, then move into practical activities or demonstrations.

You can explore, share, and adapt the materials to fit the needs of your space.

USING THIS TOOLKIT IN WORKSHOPS

This toolkit is built to support a variety of group learning environments—from classroom settings and community centers to informal living room gatherings. Each section can serve as a standalone session or be integrated into a multi-part workshop series. The modular format makes it easy to tailor discussions to different audiences based on age, digital literacy levels, or community needs. Here are ways to bring it to life in workshops:

- **Start with a Check-In:** Open with a prompt related to the section (e.g., "When was the last time you checked your privacy settings?" or "What do you think happens to your data after you close an app?").
- **Use the Reflection Activities:** Each section includes prompts that can spark personal insights and group discussions. Encourage journaling or small group sharing.
- **Facilitate Hands-On Demos:** Walk participants through privacy settings, data tracking tools, or encrypted messaging apps. Make it interactive—bring devices if possible.
- **Print and Remix Tools:** Use the checklists and exercises as printouts, handouts, or projected slides. Let participants annotate or personalize them.
- **Host Role-Plays or Scenarios:** Act out real-life tech situations (e.g., responding to a phishing scam or deciding whether to use a public Wi-Fi network) and talk through choices.
- **Build Together:** Use the Advocacy section to co-create privacy pledges, group norms for safe tech use, or strategies to support others.
- **End with a Takeaway:** Encourage participants to name one practice they'll try, one thing they'll share, or one tool they'll explore further.

NAVIGATING YOUR DIGITAL SELF TOOLKIT:

The toolkit is structured like a digital body map:

- Digital Literacy (The Brain): Core knowledge and awareness
- Digital Footprint (Your Feet & Trail): What you leave behind
- Digital Surveillance (The Eyes Watching You): Who sees you and how
- Digital Presence (Your Outer Layer): How you appear online
- Digital Advocacy (Your Armor and Voice): How you defend and strengthen your digital rights

Each part connects to the next, building a fuller picture of your digital self and how to be digitally private.

01

DIGITAL LITERACY

WHY DIGITAL LITERACY?

Your digital life is happening all the time, not just when you're scrolling or posting, but in the background of everything you do online. Before you can protect your data, defend your rights, or take action, you have to see the system.

This section is the brain of the toolkit because it's about awareness. It's about thinking critically about the systems you're inside of — the apps, platforms, and networks that shape what you see, collect your data, and influence your behavior.

Digital Literacy is the ability to critically understand, navigate, and question the digital world. Not just how you use it, but how it uses you.

This section lays the groundwork for everything else in the toolkit.

KEY TERMS

These terms will help you decode the systems you interact with every day and spot the red flags hiding in plain sight.

DIGITAL LITERACY: The ability to access, understand, critically assess, and create digital content, including recognizing how systems collect, influence, and manipulate information.

DIGITAL PRIVACY: Your right to control how your personal data is collected, used, shared, and stored online, from your photos and messages to your biometrics and browsing history.

SURVEILLANCE CAPITALISM: An economic system where companies collect your data to predict and influence your behavior, often for profit and often without your full awareness or consent. (Coined by Shoshana Zuboff)

ALGORITHMS: Sets of coded rules used by apps and platforms to decide what you see, when, and why, all based on your data and behavior.

FILTER BUBBLE: A personalized digital environment where algorithms only show you content you already agree with, limiting exposure to new perspectives.

DEFAULT SETTINGS: The pre-set options on apps, websites, or devices that often favor data collection over privacy, unless you change them manually.

THIRD-PARTY TRACKERS: External companies (not the site you're on) that collect data through plug-ins, ads, or cookies.

COOKIES: Small files stored on your device that track your behavior and remember your activity across sites.

PLUG-IN: A small tool or piece of software that adds extra features to a website or app, like comment sections, video players, ads, social share buttons, or interactive maps. They are often made by outside companies, which means that when the plug-in loads, it can collect data about you, even if you don't click anything.

TERMS & CONDITIONS: A legal agreement you accept when using a digital service that often includes hidden small clauses about data sharing, surveillance, arbitration, and more.

PRIVACY POLICY: A document that explains how a company collects, uses, stores, and shares your data (and often hides it).

FORCED ARBITRATION: A clause buried in terms & conditions that prevents you from suing a company in court, forcing you into a private process that usually benefits the company, not you.

WHAT IS DIGITAL PRIVACY?

Now that we've defined the language, let's explore one of the core concepts of digital literacy: **privacy** – what it means, why it matters, and who profits when we don't have it.

Digital Privacy is the right to control how your personal information is:

collected **used** **shared** **stored**

This includes everything from your browsing history, messages, and location to your face scans, fingerprints, and voice recordings.

This information, your digital self, is constantly being gathered by apps, platforms, and devices. But most of that happens invisibly, through systems you didn't build, can't fully see, and often didn't explicitly agree to.

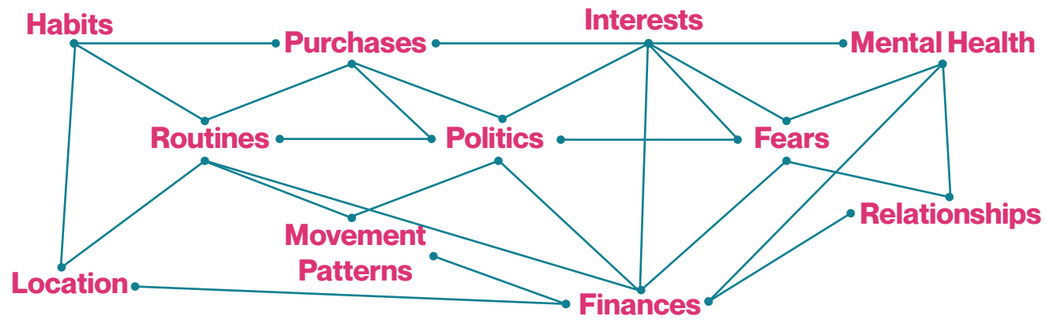
Privacy is not about hiding; its about agency.

Its about choosing what you share, when, and with whom.

It's about having boundaries, not secrets.

WHY DOES IT MATTER?

Your data is powerful because it tells a story about who you are.



WHO PROFITS?

In the wrong hands, that story can be used to manipulate, target, or harm. And that's not just hypothetical, it's happening every day:

- Tech companies profit from your data by turning it into ads, predictions, or profiles to sell.
- Governments use surveillance to monitor and sometimes suppress people, especially marginalized communities.
- Employers, landlords, insurers, and others may use your data to make decisions that impact your access to jobs, housing, or care, often without transparency.

Caring about your privacy isn't about being suspicious; it's about protecting your rights and your well-being.

HOW ARE YOU BEING TRACKED?

Even when you're not actively posting, you're being observed. Devices, platforms, and algorithms are constantly collecting data, often in the background.

Here how:

- Algorithms track what you like, click, search, and scroll past, then feed you more of it. This creates filter bubbles, limiting what you see and reinforcing existing beliefs.
- Devices like smartphones, laptops, and wearables collect data about your movement (GPS), your body (heart rate, biometrics), and your behavior (typing speed, camera use).
- Platforms monitor your interactions, who you talk to, when, for how long, and even what you pause on while scrolling.

Every swipe, like, or emoji is data.

Much of this is invisible by design, buried in default settings and long, unreadable terms & conditions.

But you can build awareness, set boundaries, and start to take back control.

BEFORE YOU CLICK "I AGREE"... TAKE A CLOSER LOOK

TOOL: Terms & Conditions Red and Green Flags

RED FLAGS TO WATCH FOR

Things that should make you pause

"We may share your data with trusted partners."
→ Who are they? What data?
🔍 Tip: Use Ctrl+F to search "third party" or "partners". If it's vague, that's on purpose.

"You agree to all future updates..."
→ Meaning: They can change the deal anytime.

"Stored as long as necessary."
→ Forever? Possibly...
🔍 Tip: Search "data retention." See if there is an option to delete or download your data.

Default-on Data Collection (Mic, Camera, Location)
→ Apps should ask, not assume.
🔍 Tip: Go to settings > privacy & security and check all data collected by your apps. Do this every time you install a new app.

Forced Arbitration
→ You're waiving your right to sue.
You won't be able to:
- Sue the Company
- Join a class-action lawsuit
- Get a public hearing.

You're stuck with:
- A private arbitrator who is picked by the company.
- No public record
- Almost no right to appeal

GREEN FLAGS TO LOOK FOR

Signs the company respects your privacy

- ☑ *Clear Plain Language*
- ☑ *You can delete or download your data*
- ☑ *Opt-in privacy settings (Not sneaky opt-out)*
- ☑ *Easy to find contact information or support*
- ☑ *Transparent data use and sharing statements*

PRO READING TIP

How to Skim Smarter

Don't read the whole thing - Scan for the key stuff.
Use Ctrl+F (computer) or "Find on Page" (mobile device) and search these words:

data · third-party · share · opt-out · delete · location · arbitration · tracking · consent · retention · partners · biometric · permissions · microphone · camera · cookies · profiling · sell · collect · terms update

02

DIGITAL FOOTPRINT

WHAT IS A DIGITAL FOOTPRINT?

Your digital footprint is the trail of data you leave behind whenever you use the internet; both the information you actively share (like posts and internet searches) and the data collected passively (like cookies, IP addresses, and location data).

This footprint includes all traces, content, and data points connected to your online activity, shaping how people, companies, and institutions perceive and treat you.

It can have lasting impacts on your privacy, security, reputation, and even your access to opportunities in areas like employment and education.

KEY TERMS

Understanding your digital footprint starts with knowing the key terms behind how data is created, tracked, and used.

VOLUNTARY DATA: The information you intentionally and knowingly provide while using digital platforms, such as an Instagram post or a subscription sign-up.

INVOLUNTARY DATA: The information collected about you without your explicit input or awareness. It's often gathered automatically in the background as you browse or interact with digital tools. Even if you didn't click "share," it's most likely shared anyway.

METADATA: Data about your data. It's secondary information embedded within digital files or communications, describing when, where, and how something was created. Metadata can reveal details like the time, location, device used, or sender and recipient, offering hidden insights into behavior, movement, and routines.

THIRD-PARTY PLUGIN: A third-party plugin is a tool or feature embedded into a website by an external company, rather than the owner of the site. These plugins, such as embedded videos, comment sections, or social media buttons, often collect user data for the third-party, even if the user does not engage with the tool directly.

API: An Application Programming Interface (API) is a set of protocols that allows different software systems to communicate and exchange data. While APIs enable convenient integration between platforms, such as connecting a map to a ride-share app, they also serve as channels through which user data is transferred, sometimes without clear user awareness or consent.

DATA BROKER: A data broker is a company that collects, aggregates, and sells personal information about individuals, often without their direct knowledge. This data is sourced from public records, digital interactions, commercial transactions, and app usage. Brokers compile detailed profiles used for marketing, insurance, credit scoring, or surveillance purposes.

INFERENCE ALGORITHM: Using patterns in digital behavior, systems can infer details like age, political views, income, and mental health, even if never directly shared. Built into platforms and ad systems, these predictive models use incomplete data to create detailed user profiles, shaping what content, services, or opportunities people see, or are excluded from, without their consent.

DIGITAL FINGERPRINTING: A tracking method that identifies and monitors users based on the unique configuration of their device and browser, such as what browser you use, your screen size, installed fonts and plugins ,and language. Unlike cookies, digital fingerprints can't be easily deleted or turned off, which makes them a powerful and hard-to-detect tracking method.

VOLUNTARY & INVOLUNTARY DATA COLLECTION

WHAT ARE YOU GIVING VS. WHATS BEING TAKEN?

VOLUNTARY

You choose to share, even if you don't always realize what you're giving up long-

Examples:

- Signing up for a newsletter
- Posting a photo publicly
- Filling out a form with your name and email
- Accepting cookies (even if you don't read them)
- Adding a location to your Instagram photo
- Uploading a video to TikTok
- Using your face to unlock your phone
- Joining a loyalty program or rewards app
- Agreeing to app permissions for convenience (like a weather app using your location)
- Taking online personality quizzes
- Commenting or liking posts on public forums or pages

INVOLUNTARY

Data collected about you, even if you never actively shared it.

Examples:

- Location tracking is running silently in the background on apps
- Bluetooth and Wi-Fi track your device as you move through stores, airports, or cities.
- Data brokers will buy and sell your personal information without consent.
- Smart TVs track what you watch and reporting it back to advertisers
- Facial recognition scanning you in public without your knowledge.
- Predictive text algorithms analyze your messages and emails.
- Keyword scanning by email providers for ad targeting, like Gmail scanning emails for product ads.

Not all data is voluntary. Some is taken without asking.

HOW IS YOUR DATA COLLECTED, STORED, & SOLD?

COLLECTION

It starts with your clicks, swipes, searches, and shares.

- Websites you visit
- Apps you download
- What you type, watch, buy, or like
- Cookies, device sensors, and location tracking
- Voice assistants listening for commands
- Even if you don't submit a form, just being online creates data trails.

STORAGE

Your data doesn't disappear, it gets saved.

- Stored in massive databases or cloud servers
- Linked to identifiers like your IP, email, or device ID
- Analyzed to build profiles about your habits, interests, and behavior.

SALE

Your digital self becomes a product. Data brokers, advertisers, and third-party companies may:

- Buy and sell your data to target you with ads.
- Share your behavior with other platforms
- Use it to influence your decisions, limit your options, or predict your actions. You rarely see it, but your information becomes someone else's profit.

You are not the customer, you are the product.
Knowing how your data moves is the first step to protecting it.

HOW IS YOUR DIGITAL FOOTPRINT BUILT?

Every click, search, and scroll adds to the file on you

DATA DETOX CHECKLIST

TOOL: De-clutter your digital trail and take back control of what you leave behind

REVIEW YOUR *VOLUNTARY* FOOTPRINT

Everything you’ve intentionally posted, shared, or signed up for.

- ☐ Google yourself - What shows up?
- ☐ Check your public social media profiles - What can strangers see?
- ☐ Delete or hide old accounts you no longer use (you can use tools like JustDelete.me)
- ☐ Unsubscribe from email lists you don’t need
- ☐ Clear out your public comment history on blogs, forums, Reddit, etc.
- ☐ Update or remove outdated bios, photos, or contact info that you no longer want out there
- ☐ Create a “burner” email for apps, contests, or one-time downloads
- ☐ Delete apps you no longer use.

QUICK SCAVENGER HUNT

Pick one file topic from the left and find a real example on your phone!

- **Voluntary Data:** Delete an old post you don’t want to be public.
- **Plug-Ins:** Spot a hidden “Like” button or embedded map.
- **Inference Algorithms:** Think about a creepy targeted ad you saw.
- **Metadata:** Check a photo for hidden location info.

REDUCE YOUR IN*VOLUNTARY* FOOTPRINT

The stuff collected passively, without your full awareness.

- ☐ Turn off location services for apps that don’t need it

  Settings > Privacy & Security > Location Services > Disable location for all apps, or Individually based on your preference.

- ☐ Disable auto-fill and saved passwords in browsers you don’t trust

  Do this in the settings of your chosen browser app

- ☐ Use Privacy-first browsers like Brave, Tor, or DuckDuckGo.
- ☐ Clear cookies and site data regularly (or auto-delete when browser closes)

  Settings > Privacy & Security > Clear Browsing Data

- ☐ Add extensions like uBlock Origin or Privacy Badger to block trackers

  These extensions block ads, trackers, and known malicious scripts, making your page load faster and preventing it from tracking you.

Small actions add up.

FIND IT. FIX IT. PROTECT YOUR FOOTPRINT

APP PERMISSIONS MAP

When you download an app, it often asks for access to different parts of your phone, like your location, contacts, microphone, camera, or even your calendar and health data. Some of these permissions are necessary for the app to function, but many are turned on by default or requested in ways that make it feel easier to say yes than to ask questions.

The truth is, by granting access, you're often giving away more than just functionality; you're giving apps insight into your daily life, your habits, and even your identity. This map breaks down the most common types of permissions apps request and why they matter.

The good news? You have the power to change most of these settings in your phone's privacy menu, but you have to know they're there first.

CONTACTS

What they get: Names, Numbers, email addresses, and social connections.
Why it matters: Apps can map your relationships, sync them to third parties, or use them for growth tactics ("invite your friends!"). You're not just giving up your privacy - you're giving up theirs too.

LOCATION

What they get: Your real-time location, past locations, travel routes, nearby Wi-Fi networks, where you've been, how often, and when.
Why it matters: Apps like ride shares need your location to work, but many keep tracking you in the background, even when you're not using them. Over time, that data can reveal patterns about your home, work, habits, routines.

CAMERA

What they get: Access to your photos and videos.
Why it matters: Some apps can activate your camera without clear consent or might continue to access it even when not in use. Apps don't need your camera unless you're actively using features like video or scanning, and even then, you can turn it on just when needed.

MICROPHONE

What they get: Audio input - potentially ambient conversation, background noise, and voice commands.
Why it matters: Some apps may be passively listening. Even if not recording, data like sound patterns can be used to guess context (like if you're in a busy place, with music, or around other voices).

CALENDAR

What they get: Events, times, locations, and attendees
Why it matters: Apps can analyze how busy you are, where you're going, who you meet with, and even what kinds of events you attend, which can be used for profiling or ad targeting.

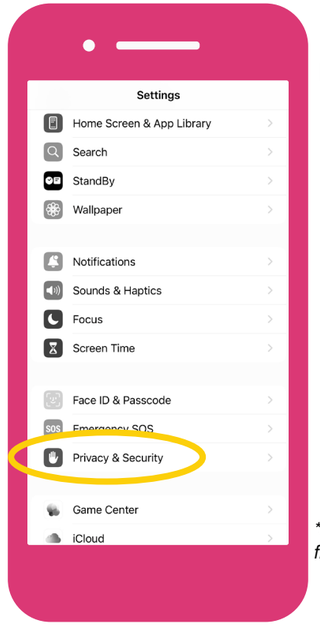
HOW TO:
MANAGE YOUR APP PERMISSIONS

IPHONE APP PERMISSIONS:

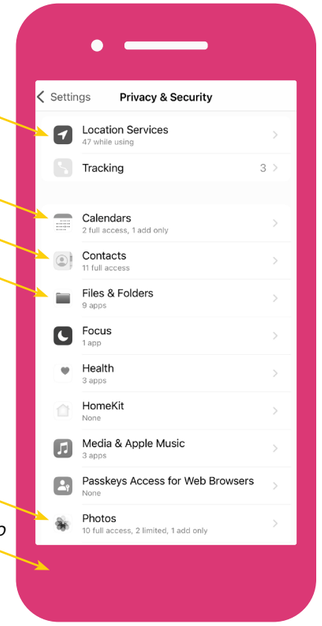
1. Go to your Settings App

2. Scroll to find Privacy & Security

3. Adjust what personal information your apps have access to



Location Services
Calendar
Contacts
Files
Photos
*Scroll down on this page to find Microphone

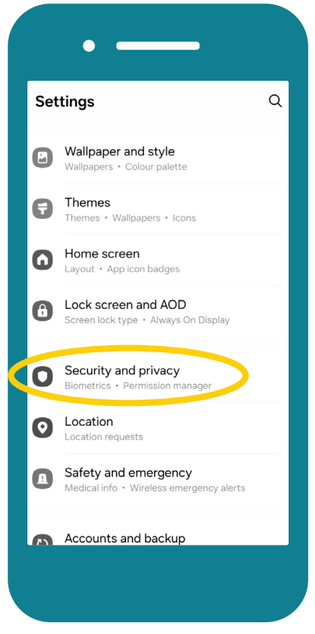


ANDROID APP PERMISSIONS:

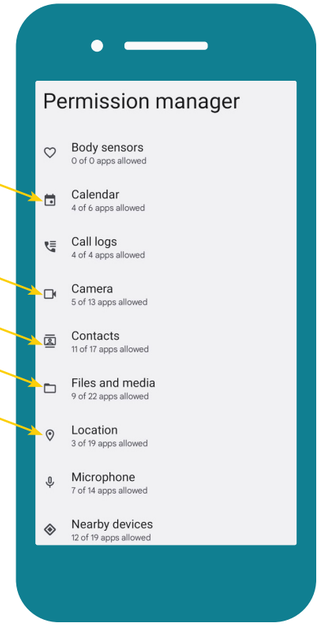
1. Go to your Settings App

2. Scroll to find Privacy & Security

3. Adjust what personal information your apps have access to



Calendar
Camera
Contacts
Files
Location Services



PROTECT YOUR ACCOUNTS

PASSWORDS, 2FA, & PASSWORD MANAGERS

Your accounts are the keys to your digital life. Strong passwords and two-factor authentication (2FA) keep your digital footprint safe from breaches, hacks, and impersonation.

CREATE STRONG, UNIQUE PASSWORDS

- Use long passwords - at least 12-16 characters
- Avoid using obvious information as your password (birthdays, pets, nicknames)
- Never use the same password across multiple sites

USE A PASSWORD MANAGER

Password managers create, store, and autofill strong, unique passwords for your accounts, so you don't have to remember them all.

How they work:

- You set one strong master password to unlock the manager
- The manager encrypts all your saved passwords, keeping them secure.
- When you log in to a website or app, the manager can autofill your password safely
- Some password managers also suggest strong passwords when you're creating new accounts

The passwords stay encrypted until you unlock them with your master password, meaning even the company that makes the manager can't see them.

Reusing passwords across accounts is risky. Password managers help you stay safe without having to memorize dozens of complex passwords.

Recommended Password Manager: Bitwarden

TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your accounts.

Even if someone steals your password, they can't get in without a second code

How to Turn on 2FA:

1. Open the app or website settings.

Look for Settings → Security → Two-Factor Authentication or Login Security.

2. Choose your authentication method.

- Authentication App (Duo Mobile, Aegis Authenticator, 2FAS): recommended method
- Text Message (SMS): less secure, but better than nothing
- Security Key or Hardware Token — a physical device for even stronger protection.

3. Follow the setup instructions.

- If using an app, scan the QR code or enter a setup key.

If using SMS, confirm your phone number.

4. Save your backup codes!

Backup codes help you get back into your account if you lose access to your phone.

The more doors you lock, the harder it is to break in.

WHAT IS ENCRYPTION?

Encryption transforms readable data (like a message or file) into scrambled code that looks like gibberish unless you have the right cryptographic key to unlock it.

HOW IT WORKS:

Plain Text → **[Encryption Key]** → **Encrypted Data**

Encrypted Data → **[Decryption Key]** → **Plain Text Again**

WHERE ENCRYPTION HAPPENS:

- Secure Websites (https)
- Messaging Apps
- Password Managers
- Email Services
- Cloud Backups
- VPNs

WHY ENCRYPTION MATTERS:

- Protects your privacy
- Secures your identity, passwords, and messages.
- Blocks hackers and unauthorized access
- Builds trust in digital communication
- Often required by law for sensitive info (healthcare, banking)

TYPES OF ENCRYPTION:

Basic Encryption: Your data is encrypted, but the service (like Google or Facebook) might still have access to the key

End-to-End Encryption (E2EE): Only the sender and recipient have the keys. No one else, not even the app, can read it.

TIPS FOR EVERYDAY PROTECTION:

- Use messaging apps with E2EE (Signal is the best option)
- Avoid syncing encrypted content to cloud services without checking settings
- Use password managers and encrypted storage.
- Keep software up to date (encryption breaks if the system is weak!)

Encryption is the foundation of digital privacy, but not all encryption protects you equally.

03

DIGITAL SURVEILLANCE

WHY DIGITAL SURVEILLANCE?

You can't see it, but it sees you. Surveillance is built into the everyday infrastructure of the digital world, from the apps on your phone to the cameras on your street. Sometimes it's marked as protection, other times it's used for control.

This section is the eyes of the toolkit, because it focuses on who is watching, why they're watching, and what that visibility does to you, psychologically, socially, and politically.

Being watched changes how we act. When surveillance becomes the norm, freedom gets blurry.

This section helps you see the watchers and decide how you want to be seen.

KEY TERMS

Surveillance relies on complexity to stay invisible. These terms give you the tools to see clearly and resist.

SURVEILLANCE CAPITALISM: An economic system where companies collect, analyze, and sell personal data, often without consent, in order to predict and influence behavior for profit. It turns human experiences into raw data used to manipulate choices, usually for advertising, control, or market advantage.

PREDICTIVE POLICING: The use of data analysis, algorithms, and artificial intelligence to forecast where crimes are likely to occur or who might commit them. It relies on historical crime data to guide law enforcement decisions, but it often reinforces existing biases and overpolicing in marginalized communities.

PREDICTIVE SEARCH: A feature where search engines or apps suggest queries, answers, or content based on your past behavior, popular trends, and algorithmic guesses about what you want.
While it can feel convenient, predictive search can limit what information you encounter, reinforce existing beliefs, and steer your choices without you realizing it.

FACIAL RECOGNITION: Technology, like facial recognition, scans and identifies faces using biometric data, often deployed in public spaces or through security systems. While it's framed as a tool for safety or convenience, facial recognition enables constant tracking, misidentification, and profiling, especially harmful to marginalized groups. Once your face is in the system, you lose control over where and how it's used.

CHILLING EFFECT: The idea that people change or suppress their behavior when they feel they're being watched, online or in person. Surveillance can discourage free expression, protest, or even harmless browsing. If you're worried about being flagged, tracked, or judged, you're less likely to speak up or explore certain topics, even when doing nothing wrong.

LICENSE PLATE READERS (LPRS): Cameras that automatically scan, record, and store license plate numbers, often placed on police cars, streetlights, or highways. These systems can track your movements in real time or over long periods, building a detailed map of where you've been. This info can be accessed by law enforcement, or sometimes even sold, without your knowledge or consent.

DATA AGGREGATION: The process of collecting and combining data from multiple sources to create a detailed profile about you. This can include your browsing history, purchases, location, and more. When pieced together, even small bits of data can reveal intimate details about your life, habits, health, relationships, or beliefs. Companies and governments can use this to target, manipulate, or monitor you without ever asking for permission.

BIOMETRIC SURVEILLANCE: The collection and tracking o biological data like fingerprints, face scans, voice patterns, and the way you talk. These identifiers are often used without consent and, once collected, are nearly impossible to change or control.

WHO IS WATCHING

Surveillance isn't just about cameras; it's the system of watchers. Some are obvious, like police cameras or airport scans. Others are hidden, like your apps silently tracking you, or platforms profiling you based on who you follow.

GOVERNMENT SURVEILLANCE

Tools Used:

- CCTV Cameras in public spaces.
- Facial recognition at airports, events, and in some public housing.
- License Plate Readers tracking your vehicle's movements
- Predictive Policing Programs
- Data sharing between police departments and private companies (like Amazon Ring)

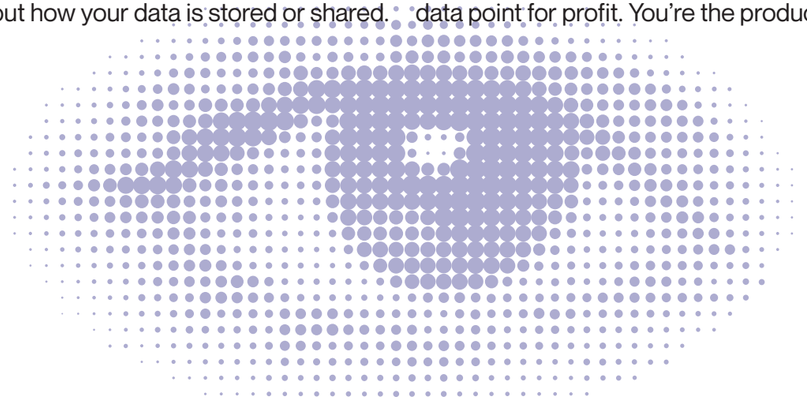
These systems can misidentify people, especially Black and Brown individuals, and are often used without community consent. They're also rarely transparent about how your data is stored or shared.

CORPORATE SURVEILLANCE

Tools Used:

- App Permissions (location, contacts, microphone, camera)
- Ad Trackers that follow you across the web
- Browser Fingerprinting that identifies your device, even with incognito mode
- Smart devices (phones, TVs, speakers, smart fridges, watches) collecting data about you and your habits constantly

Most companies harvest your data to fuel ad systems. That means everything you browse, say, and even think about (thanks to predictive search) becomes a data point for profit. You're the product.



SOCIAL SURVEILLANCE

Tools Used:

- Social media posts and tagging
- Location sharing in apps like Snapchat or FindMy
- Neighborhood watch groups and apps like Nextdoor
- Smart doorbells and home cameras

Sometimes, surveillance comes from people around you. Whether it's tagging you in posts or calling the cops over suspicion, community-based surveillance can be deeply racialized and harmful, especially when data is passed to law enforcement.

HOW SURVEILLANCE SHAPES BEHAVIOR

Surveillance doesn't just watch; it changes how people move, speak, share, and act. Even when invisible, it reshapes choices, actions, and opportunities.

CHILLING EFFECT

People hold back from expressing themselves.

- Posting less online
- Avoiding certain protests, meetings, or conversations.
- Self-restricting behaviors that might seem "risky" or "flagged"

BEHAVIOR NUDGING

People are steered toward preferred behaviors

- Accepting platform "recommendations" without questioning them.
- Changing purchases, opinions, or routines based on what algorithms
- Moving toward what feels "less risky" or "approved" by invisible systems.

SELF-POLICING

People start to monitor themselves automatically

- Editing language to sound more "neutral" or "safe".
- Altering appearance, routines, or travel patterns.
- Second-guessing normal activities in case they "look suspicious."

IDENTITY MANAGEMENT

People craft curated versions of themselves

- Presenting only certain parts of their life online.
- Hiding activism, identity markers, or affiliations.
- Adjusting how you present yourself to seem "less risky" or "more acceptable."

Recognizing how surveillance shapes behavior is the first step toward resisting it.

You still have the power to choose, create, and protect your digital self.

Every small act of awareness, every refusal to self-censor, every choice to protect your data, every effort to organize safely, pushes back against being controlled.

PREDICTIVE SURVEILLANCE

Systems that collect your data to guess and control what you might do next.

WHAT IS PREDICTIVE TRACKING?

- **Systems that analyze past behavior (your location, purchases, messages, associations) to predict what you might do next.**
- It's used by advertisers, police departments, immigration systems, insurance companies, and even employers.
- These predictions are treated like facts, even though they're guesses based on incomplete or biased data.
- You're treated like people who "look" like you.
    - Predictive systems group you based on data patterns (your zip code, race, age, friends, or online behavior) and then make guesses about who you are or what you'll do, based on what others in your "group" have done.

WHAT IS PREDICTIVE POLICING?

- **Police use data (crime reports, arrest records, surveillance feeds, social media posts) to predict where crimes might happen or who might commit them.**
- These systems often target the same neighborhoods that are already over-policed, like communities of color, low-income areas, and immigrant populations, reinforcing existing inequalities.
- People can be flagged as suspicious without committing any crime, based on who they know, where they live, or what they post.

WHY IS IT DANGEROUS?

- **Bias gets amplified.**
    - If police over-surveil certain neighborhoods, the data says "this place has more crime" because that's where arrests happen.
    - More surveillance = More "evidence" of crimes = Even more surveillance.
- **Prediction becomes punishment.**
    - People are targeted as risky or dangerous before they've done anything wrong.
- **No accountability.**
    - Most predictive systems are secretive. You often can't see, challenge, or correct the data being used against you.

EXAMPLES

- **ShotSpotter:** Sensors "detect" gunshots but are unreliable, and mostly placed in Black or Brown neighborhoods.
- **COMPAS (Software):** A risk assessment tool used in U.S. courts to predict the likelihood of someone re-offending. It often labels Black defendants as higher-risk than white defendants, even when they have similar records, leading to unfair sentencing decisions.
- **Social Media Monitoring:** Protesters flagged or investigated based on hashtags and posts.

PROTECT YOURSELF

You can't always stop surveillance, but you can make it harder, slower, and less useful.

Protecting yourself is an act of resistance.

1. SECURE YOUR DEVICES

- Use encrypted messaging apps like Signal
- Browse with privacy-focused browsers (Brave, Tor, and DuckDuckGo), and use a VPN when possible.
- Turn off location services in your phone settings when not needed.

2. MANAGE YOUR DATA

- Limit app permissions - deny camera, microphone, and location access unless necessary.
- Use strong, unique passwords and enable two-factor authentication.
- Clean up your online presence: Delete old accounts, clean up public posts, and reduce what's visible.

3. MOVE SMART

- Post about events after they happen, not during.
- Wear hats, glasses, and masks if you're worried about facial recognition.
- Use Faraday bags to block your phone's signals during protests or sensitive gatherings.

4. KNOW THE SYSTEMS

- Understand what data is collected and how it's used.
- Awareness is a form of defense.

COLLECTIVE PROTECTION & COMMUNITY CARE

Surveillance doesn’t just target individuals, it targets communities.

Protecting privacy is a collective act of care and resistance.

1 BUILD AWARENESS TOGETHER

- Host digital privacy workshops in your neighborhood, school, or community space.
- Share privacy tools and guides with friends and family.

2 SUPPORT LOCAL FIGHTS AGAINST SURVEILLANCE

- Join efforts to ban facial recognition and limit predictive policing in your city.
- Advocate for transparency laws that force agencies to reveal surveillance practices, like the POST Act NYC

3 CREATE SAFER DIGITAL SPACES

- Practice consent online
  - Before sharing photos, locations, or tagging others, ask permission.
- Encrypt group chats and use safer collaboration tools.
- Organize mutual aid tech teams: people helping each other secure their devices, accounts, and data.

4 WATCH OUT FOR EACH OTHER

- Document surveillance harms
  - If you see someone being targeted, record responsibly and protect them.
- Educate without shaming
  - Help people improve their privacy without blame, especially those new to it

04

DIGITAL PRESENCE

WHAT IS A DIGITAL PRESENCE?

How you appear online isn't just about what you post; it's what platforms decide to show, what algorithms amplify, and what others assume. Your digital presence is shaped by both design and data, choice, and automation.

This section is the skin of the toolkit, the outer layer of what people, platforms, and systems see when they encounter you online. It's about perceptions, visibility, and power.

You're not just using the Internet. You're being interpreted by it.

This is different from your digital footprint, which focuses on the trails you leave behind — often invisible, involuntary, and tracked in the background. Digital presence, by contrast, is what's visible. It's your digital reflection: what's seen, searchable, and often curated (even when you don't realize it).

This section helps you take back control of your digital reflection; not to perform, but to protect and present yourself on your terms.

KEY TERMS

Your digital world is built on invisible rules. These terms give you the tools to recognize, question, and resist them.

ONLINE IDENTITY: Similar to your digital presence, this is the version of you that exists across the Internet, shaped by your posts, profiles, search history, purchases, and even what others share about you.

ALGORITHMIC BIAS: When automated systems, like recommendation engines or AI tools, produce unfair discriminatory results. This is because they are usually trained on biased data or reflect the values of their creators. Bias in algorithms can lead to unequal treatment in everything from job ads and loan approvals to policing and content moderation. Even if the bias isn't intentional, it can still reinforce stereotypes and deepen existing inequalities.

PLATFORM CURATION: The way digital platforms, like Instagram, TikTok, or YouTube, choose what content to show you is platform curation. This is usually driven by algorithms designed to keep you engaged. These curated feeds can trap you in filter bubbles, limit what perspectives you see, and subtly shape your beliefs or moods. What shows up isn't neutral; it's optimized for clicks, not trust or well-being.

ENGAGEMENT METRICS: Measurements of how users interact with content, like likes, shares, comments, watch time, and clicks. Platforms use these metrics to decide what to promote or hide. This means that emotional, extreme, or addictive content often gets pushed to the top, even if its misleading or harmful. Your attention becomes the product.

SHADWOBANNING: When a platform secretly limits your visibility, like hiding your posts or reducing reach, without telling you. You might keep posting, unaware that others aren't seeing your content. Shadowbanning can silence activism, suppress marginalized voices, or punish users without transparency or accountability.

IMPRESSION MANAGEMENT: The way we try to control how others see us, especially online, where we curate posts, photos, bios, and more to shape a certain image. Social platforms encourage constant self-performance, rewarding curated versions of ourselves over authenticity. This can lead to pressure, burnout, and a disconnect between who you are and who you feel you need to be online.

FILTER BUBBLE: A situation where algorithms show you only the content that aligns with your existing beliefs or interests, trapping you in an echo chamber. Filter bubbles limit exposure to diverse perspectives and can make it harder to find unbiased information.

ECHO CHAMBER: When your digital environment (friends, news feeds, forums) mainly reflects your own views, reinforcing beliefs without challenge. While comforting, echo chambers can deepen polarization and reduce critical thinking.

WHY DOES YOUR DIGITAL PRESENCE MATTER?

Your digital presence shapes how you are seen, understood, and treated, not just by people, but by platforms, governments, and algorithms.

It influences your opportunities, your safety, and even your rights.

Everything you post, react to, and connect with online builds a public version of you, sometimes intentionally, sometimes without your control.

Even things you don't post yourself, like tagged photos or search engine results, contribute to the image the digital world creates about you.

Managing your digital presence isn't about being invisible; it's about being intentional with the parts of yourself you share, and how you navigate a system built to watch, sort, and profit from you.

INTENTIONAL PRESENCE

- What you post
- Profiles and Bios
- Shared photos and videos
- Comments and likes
- Public accounts

UNINTENTIONAL PRESENCE

- What others post about you
- Tagged photos
- Online search results
- Profiles you forgot about
- Algorithmic targeting

FINDING THE BALANCE
SELF-EXPRESSION VS. PRIVACY

1. SHARE INTENTIONALLY, NOT IMPULSIVELY

Ask yourself:

- Who needs to see this?
- Would I be comfortable if it resurfaced later?
- Am I sharing for connection or for validation?
- Could this information be misused?

2. CONTROL YOUR AUDIENCE

Use private accounts, close friends lists, and custom visibility settings to limit who can see your posts.

3. PROTECT SENSITIVE INFORMATION

Avoid sharing real-time locations, daily routines, personal IDs, and sensitive personal details.

4. SEPARATE YOUR PUBLIC & PRIVATE SPACES.

Treat your online presence like different rooms:

- Public profiles (like LinkedIn or a professional portfolio) are for wide audiences.
- Private spaces (like group chats, alternate accounts, or close friends lists) are for personal sharing.

5. OWN YOUR BOUNDARIES UNAPOLOGETICALLY

Privacy isn't about secrecy, it's about protecting what matters most to you.

BEFORE YOU POST

- Check privacy settings
- Be mindful of hidden info
- Share for yourself, not validation

SOCIAL MEDIA PRIVACY 101

STAY CONNECTED. STAY PROTECTED.

Social media helps you connect, create, and organize, but it also tracks, collects, and exposes you.

Protecting your privacy doesn't mean disappearing. It means taking control of what you share, who sees it, and how platforms use it.

QUICK PRIVACY WINS

- ☐ Secure your social media accounts by making them private and limit visibility.
- ☐ Turn off Location Services & Review App Permissions. Limit what each app can access
- ☐ Limit personal information in bios (birthdays, schools, workplaces)
- ☐ Use strong, unique passwords + enable two-factor authentication

1. Open your Phone Settings (not the app itself)

2. Go to Privacy → Location Services & App Permissions

3. Scroll to the app you want to change (Instagram, Facebook, etc)

4. Adjust Permissions:

- *Set Location Access to: Never, or Ask Every Time*
- *Review App Access to:*
  - *Camera*
  - *Microphone*
  - *Contacts*
  - *Photos/Media*
  - *Bluetooth/Nearby Devices*

Turn OFF access to any app that doesn't need it.

REVIEW YOUR SETTINGS REGULARLY, PLATFORMS CHANGE!

SECURE YOUR SOCIAL MEDIA

FACEBOOK

1. Go to: Settings & Privacy → Settings.

2. Find "Privacy Checkup" under Tools & Resources.
(It's a shortcut to help you.)

3. Click: "Who can see what you share?"
Start reviewing what's public about you.

4. Walk through each step:

- *Check what personal info is visible (like phone number, email, birthday).*
- *Choose what you want to hide, limit to friends, or delete.*

5. Set who can see your future posts.

- *Best options: Friends or Only Me, not Public.*

6. Save your changes.

INSTAGRAM

1. Tap your profile picture in the bottom right corner.

2. Press the three lines in the top right corner.

3. Select "Settings and Privacy."

4. Scroll down to "Account Privacy."
(You'll find options about who can view your posts.)

5. Toggle ON "Private Account."

LINKEDIN

1. Go to Settings and Privacy → Visibility

2. Set Profile Viewing to Private Mode

3. Limit what's public in Edit Public Profile

4. Restrict who can find you by email/phone

X (formerly Twitter)

1. Tap your profile picture in the top left corner.

2. Select "Settings and Privacy."

3. Go to "Privacy and Safety."

4. Tap "Audience and Tagging."

5. Toggle ON "Protect your posts" and "Protect your videos."
(Only approved followers will be able to see your posts and videos.)

6. (Optional) Turn OFF "Photo Tagging."
This prevents strangers from tagging you in photos.

TIKTOK

1. Tap your profile icon at the bottom right.

2. Tap the three lines in the top right corner to open your settings.

3. Select "Settings and Privacy."

4. Tap "Privacy."

5. Toggle ON "Private Account."
Only people you approve can follow you and watch your videos.

SNAPCHAT

1. *Tap your Bitmoji → Settings*

2. *Scroll to Privacy Controls*

3. *Set:*
   - *See My Location: Toggle ON Ghost Mode*
   - *View My Story: Friends or Custom*
   - *Contact Me: Friends*
   - *Quick Add: Toggle OFF Show Me in Quick Add*
   - *Activity Indicator: Toggle OFF*

05

DIGITAL ADVOCACY

WHY DIGITAL ADVOCACY?

Awareness is important, but action is necessary. The systems shaping our digital lives aren't inevitable or neutral, and have the right to question, resist, and re-imagine them.

This section is the hands of the toolkit. The part that builds, resists, and defends. Digital advocacy is about pushing for safer, more equitable, and more transparent technologies through education, organizing, and policy.

Privacy is not just a personal issue. It's a collective one.

This section equips you to take action. For yourself, and your community.

KEY TERMS

Key concepts to build power, protect privacy, and push for change.

DIGITAL FOOTPRINT: The record of everything you do online, including posts, searches, location data, and device use. Your digital footprint shapes how companies, governments, and others see you, and understanding it helps your protect your privacy and limit tracking.

PRIVACY RIGHTS: Your legal and ethical right to control who can access your personal information, how it's used, and where it's shared, online and offline. Privacy rights protect you from invasive data collection, surveillance, and misuse. But not all countries or platforms treat these rights equally, so knowing them, and how to advocate them, is key to digital autonomy.

DATA JUSTICE: The idea that data should be collected and used fairly, transparently, and with respect for people's rights, especially those most vulnerable to harm. Its about shifting power away from corporations and toward the people most affected by digital systems.

SURVEILLANCE RESISTANCE: The act of pushing back against the systems that monitor, track, or collect data about you, whether through tools, behaviors, or collective action. Surveillance resistance is about reclaiming control. It can look like using encryption, masking your digital footprint, or organizing for policy change. It empowers individuals and communities to protect their privacy and challenge unique systems.

ENCRYPTION: A method of protecting data by converting it into a code that only someone with the right key can read. It keeps messages, files, and personal info safe from hackers, corporations, and governments.

DIGITAL ORGANIZING: Using online tools like social media, group chats, or email to mobilize people, build community, and push for change. It connects movements across distances but also comes with privacy risks, so knowing your privacy tool matters.

POLICY ADVOCACY: The process of influencing laws, regulations, or public policies to create systemic change, often through campaigns, lobbying, research, or community action. Policy advocacy turns personal or local concerns into public change. It gives communities a voice in shaping digital rights, privacy protections, and tech accountability, shifting power from corporations and institutions to the people.

YOUR DIGITAL RIGHTS

In New York, some laws already exist to help you protect your privacy. Others are still being debated. This page breaks it down.

LAWS THAT PROTECT YOU RIGHT NOW

NY SHIELD ACT
(Stop Hacks and Improve Electronic Data Security)

- Requires businesses to protect your personal data and tell you if its been exposed in a breach.
- It expands what counts as private info and forces companies to follow strong security practices to keep it safe.

PPPL
(Personal Privacy Protection Law)

- Gives you the right to see, fix, or limit the personal data New York State agencies collect about you.
- It makes sure the government only collects info that's truly needed, and protects it from being misused or shared without your consent.

ISPA
(Internet Security and Privacy Act)

- Limits how New York State websites can collect or share your personal information. You have to give consent first.
- Gives you the right to see what info the state has on you and ask for corrections if needed, as long as it's safe to do so online.

As of May 2025, both the SAFE for Kids Act and the NY CDPA have been signed into law but are not yet in effect. They are set to be enforced starting June 20, 2025.

LAWS COMING SOON

NYPA
(New York Privacy Act)

- Would give you the power to see, correct, delete, or stop the sale of your personal data, and make companies get your clear permission to use it.
- Would hold businesses accountable with strict rules on data use, security, and transparency, aiming to treat privacy as a basic right, not a loophole.
- *NYPA has passed the State Senate but is still waiting for approval in the Assembly. It hasn't become a law yet, but advocates are pushing hard to make it real.*

NY HIPA
(New York Health Information Privacy Act)

- Would ban the sale of consumer health data and limit its use to specific, consented, or legally necessary purposes.
- Passed by the legislature in January 2024, the bill is now awaiting the governor's signature to become a law.

SAFE for Kids Act
(Stop Addictive Feeds Exploitation)

- Aims to curb the mental health harms of social media by banning addictive algorithmic-driven feeds for users under 18 without parental consent.
- Would restrict late-night notifications to minors.

NY CDPA
(New York Child Data Protection Act)

- Would ensure that online privacy is the default for anyone under 18, prohibiting websites from collecting, sharing, or processing their personal data, safeguarding kids from lifelong digital surveillance.

KNOW YOUR RIGHTS

Your current legal protections.

1 RIGHT TO DATA SECURITY
You are protected under the NY SHIELD ACT

Businesses must:

- Protect your private data (Names, emails, biometric info, financial data).
- Notify you if your data is breached or stolen, quickly and clearly.

This applies to any company holding New Yorkers' private info, even out-of-state companies.

2 RIGHT TO ACCESS & CONTROL YOUR DATA
You are protected under the Internet Security & Privacy Act (ISPA)

You can:

- Request access to personal data held by New York State agencies.
- Ask for corrections if your information is wrong.
- Know why your data is being collected, how it's used, and who it's shared with.

3 RIGHT TO LIMIT DATA COLLECTION
You are protected under the Personal Privacy Protection Law (PPPL)

State Agencies must:

- Only collect the minimum personal data needed to do their job.
- Tell you what they're collecting and why.
- Give you access to see and fix your records.

4 RIGHT TO BE NOTIFIED OF A BREACH
You are protected under the NY SHIELD ACT

You must be:

- Informed quickly if your private information is exposed in a data breach.
- Notified even if the company is based outside New York, as long as it holds your data.

5 RIGHT TO ONLINE SAFETY FOR KIDS (AS OF JUNE 2025)
You will be protected under the SAFE for Kids Act and NY CDPA.

Starting June 2025:

- Social media platforms must get parental consent before showing personalized feeds to users under 18.
- Apps and websites cannot collect, share, or sell children's personal data without clear limits.

SAFE PROTESTING
IN A DIGITALLY NETWORKED WORLD

BEFORE YOU PROTEST

Use Secure Communication Tools:

- Use Signal for end-to-end encrypted messaging, not Instagram DMs or iMessages.
- Avoid WhatsApp (Owned by Meta). It is encrypted, but metadata (who, when, where) is still visible.
- Disable cloud backups because they make encrypted messages retrievable.

Use a Faraday bag or phone pouch:

- A Faraday bag blocks all wireless signals, which means no GPS, Bluetooth, Wi-Fi, or cellular tracking.
- Use it when traveling to/from a protest or organizing site to prevent real-time tracking.

Prep your Phone:

- Disable Face/Touch ID; Law enforcement can't force you to unlock with a fingerprint or face, but they can compel a passcode in some states.
- Turn off location tracking (Settings > Privacy & Security > Location Services).
- Log out of social media or use burner accounts with minimal identifying information.
- Keep your device on airplane mode or off if you don't need it on.

ORGANIZING ONLINE

Protect Group Spaces:

- Use end-to-end encryption platforms
- Avoid organizing in Facebook groups or Discord.
- Share links to documents through privacy-friendly tools (ex: CryptPad, Riseup, ProtonDrive)

Anonymize Identities:

- Use aliases or first names only. Avoid linking to personal accounts or emails.
- Consider creating temporary organizing accounts with privacy browsers, like Tor or Brave

Use a VPN or Tor

- A VPN hides your IP address and encrypts your traffic
- Tor Browser is even more private; use it to access organizing sites or share resources.

WHILE YOU PROTEST

Limit Digital Exposure:

- Leave your phone at home, bring a burner phone, or use airplane mode.
- If you must take your phone, keep it in a Faraday bag unless absolutely needed.

Watch What You Post:

- Avoid live-streaming others or sharing identifying images
- Blur faces using tools like Signal's blur tool or the pixelate app.
- Don't geotag locations or post in real time. Wait until you're safely away, and remove any details that could reveal your or others' location or identity.

Disable Biometrics and Auto-Backup

- Disable auto-backup to iCloud services or Google Photos backup. *(Iphone: settings > Apple ID > iCloud > Photos, toggle off) (Android: Google Photos App > tap your profile picture > Photos Settings > Backup, toggle backup OFF)*
- Turn off biometric unlocking and use a strong passcode only.

AFTER YOU PROTEST

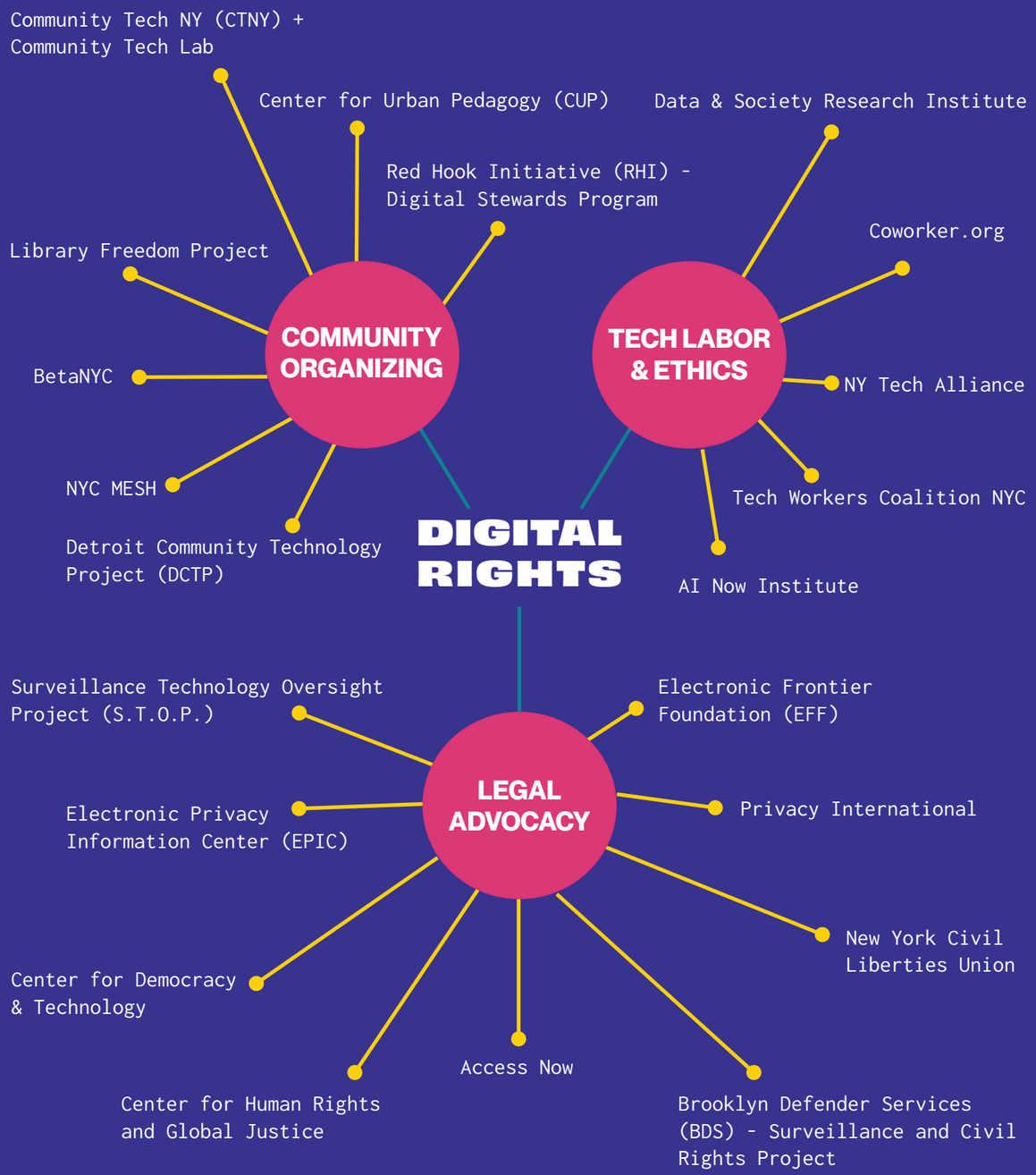
Clean your digital footprint:

- Delete unnecessary messages or files from your phone.
- Clear browser history and uninstall unused apps.
- If you were arrested or believe your data may have been accessed, reset passwords and check app/device permissions.

KNOW YOUR RIGHTS

- You have the right to film police in public, but don't interfere or get too close.
- Police need a warrant to search your phone, but they may pressure you. Stay silent and ask for a lawyer.
- Make sure your device is encrypted (iPhones and Androids are encrypted by default when you set a passcode)

THE ECOSYSTEM OF DIGITAL RESISTANCE



GET INVOLVED

FIGHT FOR YOUR DIGITAL RIGHTS

SUPPORT ORGANIZATIONS

- Donate or volunteer skills
- Attend events and workshops
- Share and amplify their work

ADVOCATE FOR STRONGER LAWS

- Call or email your local representatives
- Show up to public hearings or town halls
- Sign petitions and write letters.
- Support bills like the NY Privacy Act, SAFE for Kids, and others when they come up.

EVERY ACTION BUILDS THE ECOSYSTEM

PROTECT YOUR COMMUNITY

- Host digital safety workshops
- Help others set up safer devices and accounts
- Create mutual aid groups that include tech support
- Share emergency digital security tips

BUILD ALTERNATIVE SYSTEMS

- Join or support community Wi-Fi networks like NYC Mesh
- Use privacy-respecting apps and tools
- Advocate for public internet access.

ORGANIZE AT WORK

- Join or start a tech workers group
- Push for ethical tech policies
- Protect whistleblowers and unionize

EDUCATE OTHERS

- Host “Know Your Rights” sessions
- Make zines, infographics, or toolkits
- Mentor others on privacy and security