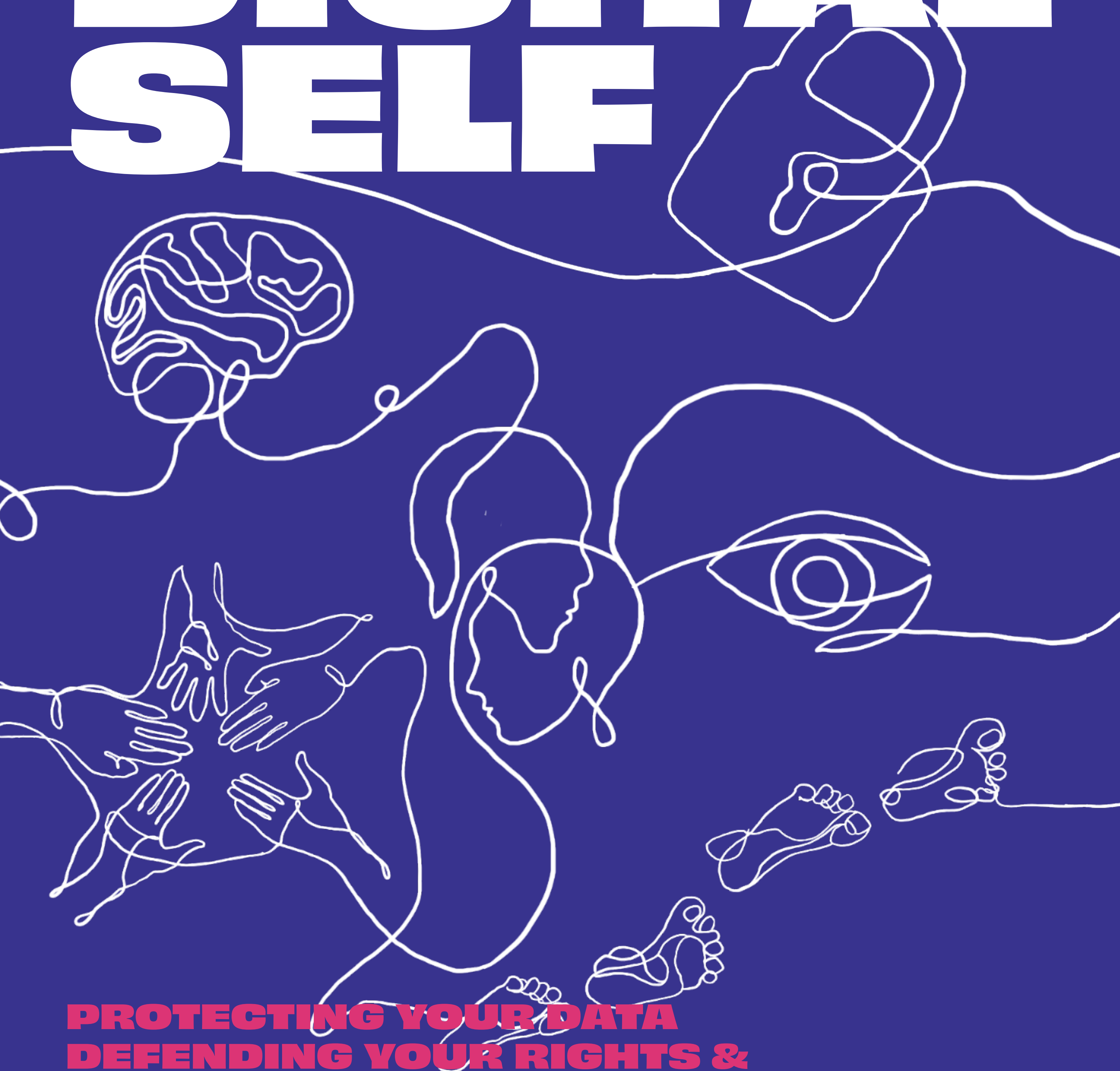
UNDERSTANDING YOUR DIGITAL SELF



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

LITERACY

FOOTPRINT

SURVEILLANCE

PRESENCE

ADVOCACY

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.

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)

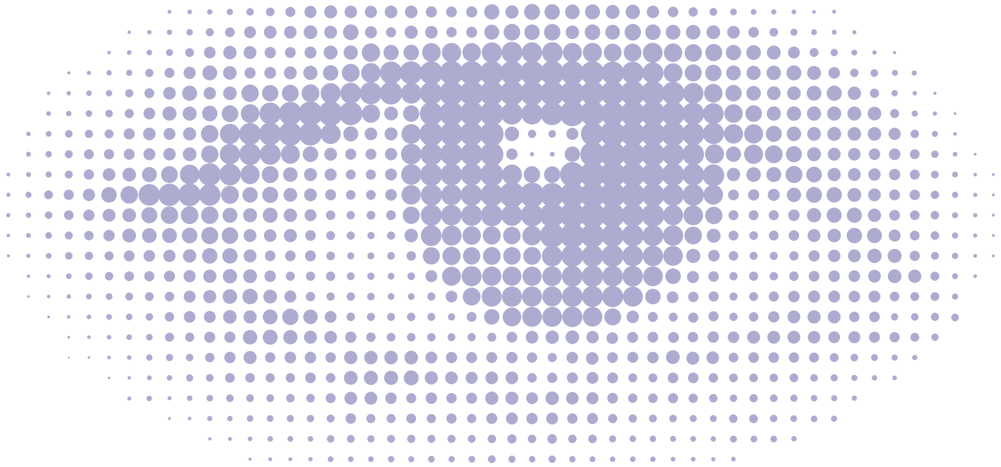
These systems can misidentify people, especially Black and Brown individuals, and are often used without community consent. They're also rarely transparent about how your data is stored or shared.

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