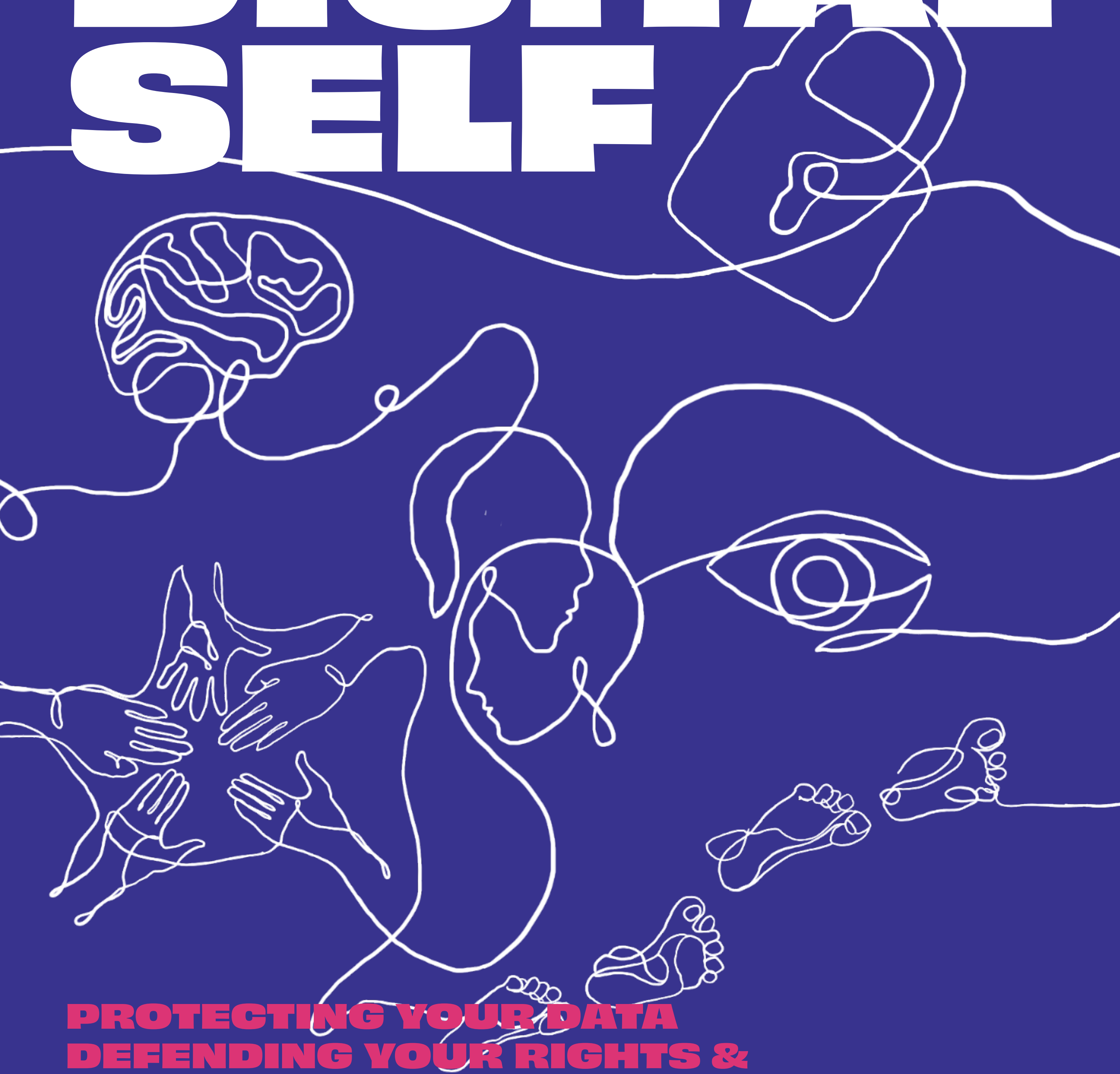
UNDERSTANDING YOUR DIGITAL SELF



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.

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.

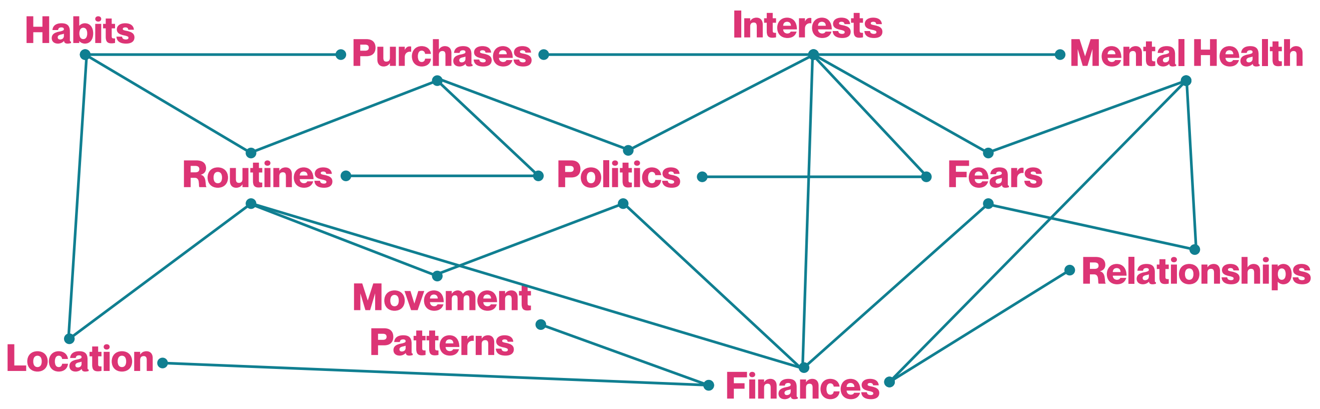
Privacy is not about hiding; its about agency.

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.

"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.

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

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