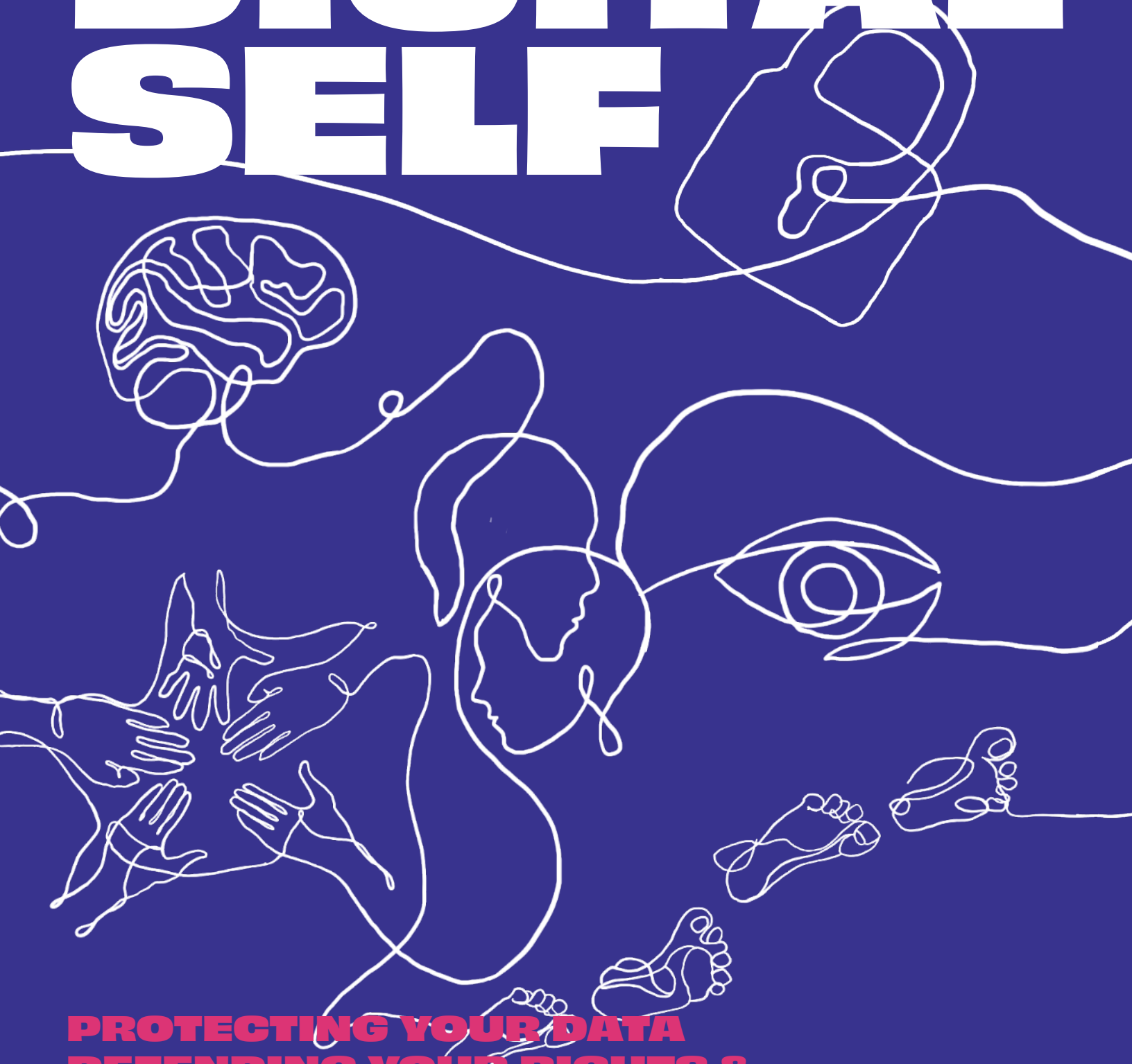
UNDERSTANDING YOUR DIGITAL SELF



**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.

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*