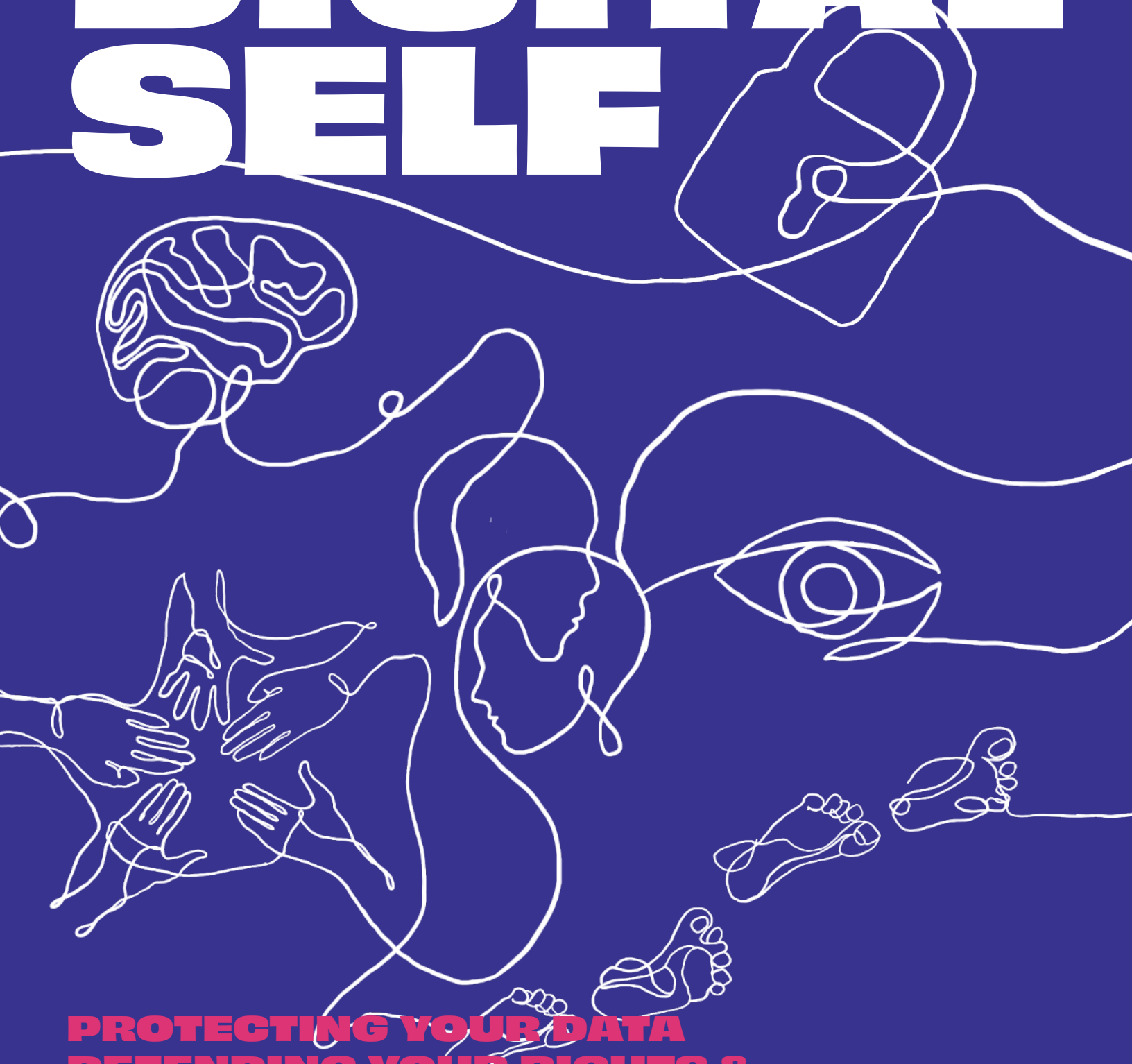
UNDERSTANDING YOUR DIGITAL SELF



**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.

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

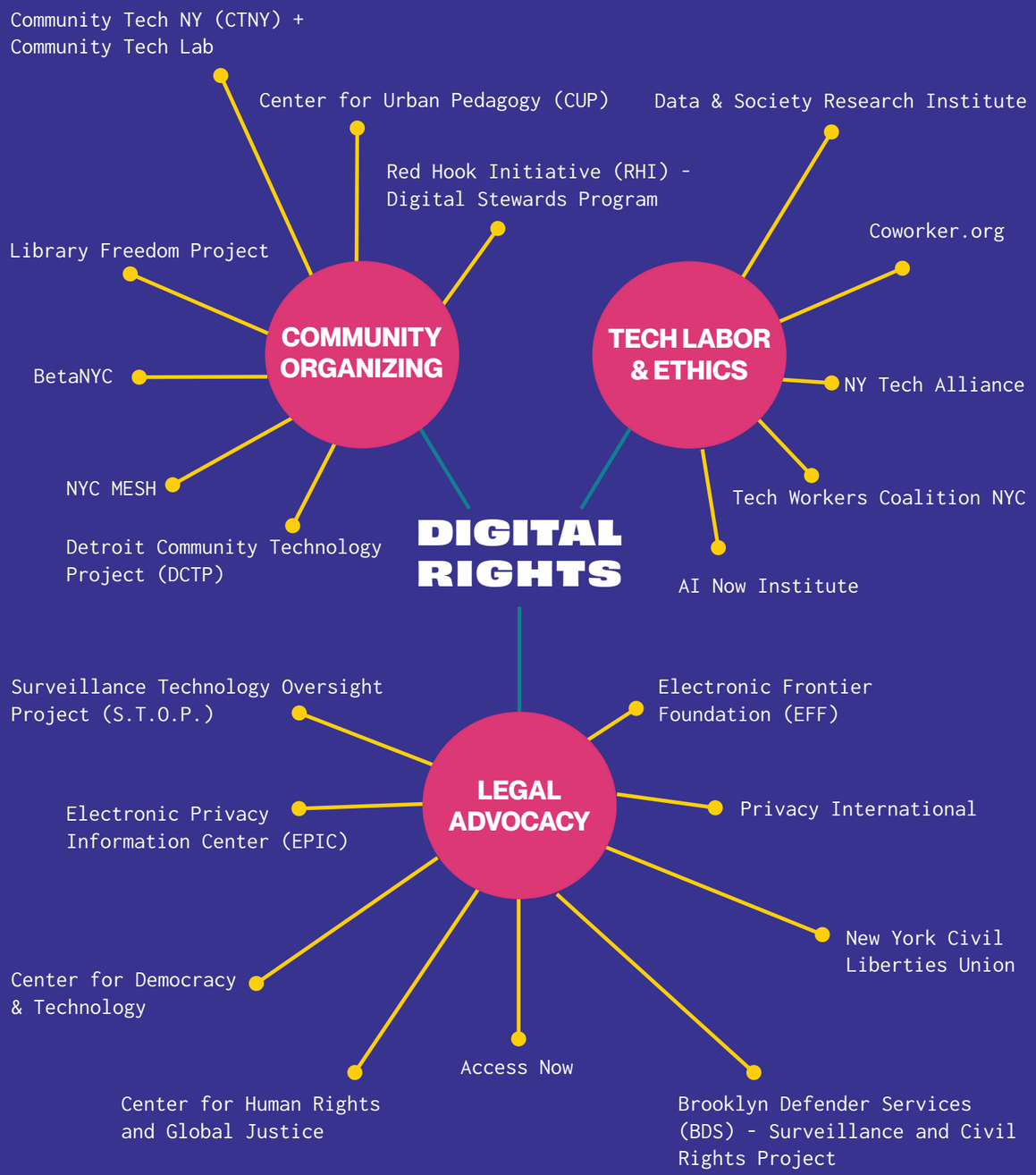
Clean your digital footprint:

- 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