

A futuristic, rainy cityscape at night. The scene is dominated by vertical neon lights in shades of pink, purple, and blue. In the foreground, a person wearing a dark tactical jacket and a large backpack stands with their back to the camera, looking out over the city. The rain is visible as vertical streaks throughout the scene. In the background, there are tall buildings, a flying drone, and various digital displays and advertisements. The overall atmosphere is gritty and cyberpunk.

WELCOME TO THE RESISTANCE

DIGITAL DISOBEDIANCE GUIDE

Digitally Disobey

A Manifesto of the Digital Freedom Movement



INTRODUCTION: THE WATERFALL

The Illusion of Choice

You clicked "Reject All" on the cookie banner. You think you said "No." **You didn't.** That button is a performance. It stops a few ad scripts from loading in your browser. It does **not** stop your ISP from logging every domain you visit. It does **not** erase the data brokers who already sold your location history, purchase history, and device fingerprints to the highest bidder. It does **not** stop the government from buying that data from a third party because they couldn't be bothered to get a warrant.

You are not "opting out." You are just wearing a blindfold while the surveillance state maps your life.

The rabbit hole goes deeper than the browser. It goes into your phone's operating system, your router, your financial transactions, and the metadata of every call you make. The "No" you clicked was a lie. The only real "No" is the one you take back into your own hands.

The Goal: Reclaiming the Internet

The internet was built to be a place of connection, not a factory for surveillance. It was meant to be open, decentralized, and owned by its users. Today, it is commercialized, walled-off, and mined for data.

Our goal is to take it back. Not by destroying it, but by reclaiming it. By building our own walls, cutting our own tethers, and changing the rules that allow this to happen.

The Path: From Awareness to Sovereignty

This booklet is not a course. It is an exit plan.

- **Right Now:** Stop the bleeding. Take immediate steps to protect yourself.
- **This Week:** Build your walls. Harden your devices and communications.
- **This Month:** Cut the tethers. Disconnect from the systems that track you.
- **The Hard Sell:** Go sovereign. Take full control of your operating system.
- **The Long Game:** Change the rules. Organize, advocate, and reclaim the internet for everyone.

You are not a user. You are not a data point. You are not a product. **You are the resistance. Now act like it.**

CHAPTER 1: RIGHT NOW (STOP THE BLEEDING)

The Reality Your phone is a tracking device you carry willingly. Your browser is a witness. Your email is an open book. Every corporation and government agency that wants your data is taking it, right now, because you haven't told them no.

Do these five things today:

1. **Install Firefox and uBlock Origin.** Chrome is Google's surveillance tool. Safari is Apple's. Edge is Microsoft's. They all report back to their parent companies. Firefox is the only major browser that isn't owned by an ad-tech giant. uBlock Origin kills the trackers, scripts, and web bugs that cookie banners pretend to manage. Stop asking permission. Block them.
2. **Change your DNS to Quad9.** Your ISP sells your browsing history. Cut them out. This takes two minutes.
3. **Get Bitwarden or KeePassXC.** You reuse passwords. You know you do. One breach and everything burns. Fix it now.
4. **Open a Proton Mail or Tuta account.** Your current email provider reads your mail. Start migrating what matters.
5. **Turn on 2FA everywhere that counts.** Email, banking, password manager. SMS is weak — use an authenticator app at minimum.

Then tell someone. You just did five things most people don't know exist. One conversation multiplies your impact. *"Hey, I just switched my browser — did you know Chrome and Safari and Microsoft Edge track everything?"*

HOW-TO SHEET A:

HOW TO INSTALL FIREFOX + UBLOCK ORIGIN

Step 1: Download Firefox

1. Open your current browser.
2. Go to mozilla.org/firefox.
3. Click "Download Firefox."
4. Run the installer. Follow the prompts.
5. Once installed, open Firefox.

Step 2: Install uBlock Origin

1. In Firefox, press **Ctrl+Shift+A** (or **Cmd+Shift+A** on Mac) to open the Add-ons Manager.
2. In the search bar, type "uBlock Origin".
3. Look for the result by "Raymond Hill" (or "gorhill"). It has a red shield icon.
4. Click "Add to Firefox."
5. Click "Add" in the confirmation popup.
6. You are now protected. The red shield icon in your toolbar means it is active.

Step 3: Verify

1. Go to browserleaks.com/javascript.
2. You should see a green checkmark saying "No JavaScript detected" or similar.
3. If you see a list of scripts, uBlock Origin is working.

Troubleshooting:

- If the page doesn't load, check your internet connection.
 - If uBlock Origin isn't blocking, make sure it's enabled in the toolbar (right-click the toolbar and ensure it's checked).
-

HOW-TO SHEET B:

HOW TO CHANGE YOUR DNS TO QUAD9

Why? Your ISP logs every site you visit. Quad9 blocks malicious sites and doesn't log your history.

Option 1: Change on Your Computer (Windows/Mac/Linux)

1. Open your Network Settings.
 - **Windows:** Settings > Network & Internet > Status > Change adapter options.
 - **Mac:** System Preferences > Network.
 - **Linux (Pop!_OS):** Settings > Network > Gear Icon > IPv4.
2. Find your active connection (Wi-Fi or Ethernet).
3. Look for "DNS" or "Name Servers."
4. Change from "Automatic" to "Manual."
5. Enter the primary DNS: 9 . 9 . 9 . 9
6. Enter the secondary DNS: 149 . 112 . 112 . 112
7. Save and reconnect.

Option 2: Change on Your Router (Recommended for all devices)

1. Open your browser and go to your router's IP (usually 192 . 168 . 1 . 1 or 192 . 168 . 0 . 1).
2. Log in (check the sticker on your router for the default username/password).
3. Find "WAN" or "Internet" settings.
4. Look for "DNS Server" settings.
5. Enter 9 . 9 . 9 . 9 and 149 . 112 . 112 . 112.
6. Save and reboot the router.
7. All devices on your network are now protected.

Verify: Go to dnsleaktest.com and run a "Standard Test." You should see "Quad9" listed as your DNS provider.

CHAPTER 2: THIS WEEK (BUILD YOUR WALLS)

The Reality Stopping the bleeding is just the first step. Now you need to build walls. Your data isn't just collected; it's aggregated, packaged, and sold. Data brokers have a dossier on you. Your phone number links your identity to your location, your purchases, and your contacts. Your carrier logs every call you make. Your disk is readable by anyone who physically holds your device. If you don't lock these doors, the surveillance state walks right in.

Do these five things this week:

1. **Move to LibreWolf or Tor.** Firefox is good, but it still phones home with telemetry. LibreWolf is Firefox stripped of all tracking and telemetry. Tor makes your traffic untraceable. If you're researching sensitive topics, your browser shouldn't be a witness.
2. **Order a YubiKey.** Authenticator apps live on your phone. If your phone is compromised, so is every account tied to it. A hardware key can't be phished, cloned, or stolen remotely. It is the gold standard for security.
3. **Encrypt your disk.** Veracrypt for Windows/Mac. LUKS for Linux. If someone takes your machine, they get nothing but a black screen. Your data stays locked.
4. **Strip your phone.** GrapheneOS if you have a Pixel. F-Droid either way. Remove the Google services that report your every move. Your phone is the most invasive device you own—tame it.
5. **Switch your calls and texts to Signal or Cape.** Your carrier logs every number you contact and when. Standard calls and texts are interceptable. Encrypted comms mean the metadata dies at your device.

Then teach someone. Show a family member how to install Signal. Help a coworker set up 2FA. Every person you pull out of the water weakens the current for everyone else.

HOW-TO SHEET C:

HOW TO SET UP BITWARDEN / KEEPASSXC

Why? Reused passwords mean one breach exposes everything. Your email, bank, and identity are one leaked database away from compromise. A password manager makes each account a separate lock.

Option A: Bitwarden (Cloud - Easier for most)

1. **Create an Account:** Go to bitwarden.com. Click "Get Started." Enter your email and create a **Master Password**.
 - *CRITICAL:* This password is the key to your kingdom. If you lose it, you lose everything. Write it down and store it in a safe place. Do not forget it.
2. **Install the Extension:** In your browser (Firefox/Chrome), go to the extension store. Search "Bitwarden." Install the official extension.
3. **Log In:** Click the Bitwarden icon. Log in with your email and Master Password.
4. **Import Old Passwords:** If you have passwords saved in your browser, go to Settings > Import Data. Select your browser and import.
5. **Start Using:** When you log into a site, Bitwarden will ask to save the password. Click "Save." Next time, it will auto-fill.

Option B: KeePassXC (Local - Maximum Privacy)

1. **Download:** Go to keepassxc.org. Download the installer for your OS.
2. **Create Database:** Open KeePassXC. Click "New Database."
3. **Set Master Password:** Create a strong password. **Save the database file (.kdbx)** to a secure location (like an

encrypted USB drive).

4. **Add Entries:** Click "Add Entry." Enter the website URL, username, and password.
5. **Browser Integration:** Install the "KeePassXC-Browser" extension. Connect it to your database in the extension settings.
6. **Backup:** Back up your .kdbx file to a second location (e.g., a cloud drive or external hard drive). If you lose this file, you lose your passwords.

Verification: Try logging into a site you use often. The manager should fill it in automatically. If it doesn't, check the extension settings.

HOW-TO SHEET D:

HOW TO ENABLE 2FA WITH AN AUTHENTICATOR APP

Why? Without 2FA, a stolen password is a free pass into your life. SMS 2FA is vulnerable to SIM swapping (hackers tricking your carrier into giving them your number). Authenticator apps are the minimum standard. Hardware keys are the goal.

Step 1: Install the App

1. Download **Authy**, **Aegis**, or **Raivo** (iOS) from your app store or F-Droid.
 - *Recommendation:* **Aegis** (Android) or **Raivo** (iOS) are open-source and secure. **Authy** is popular but closed-source.

Step 2: Enable 2FA on a Critical Account (e.g., Email)

1. Log into your email account (Proton, Gmail, etc.).
2. Go to **Security Settings**.
3. Look for "Two-Factor Authentication" or "2-Step Verification."
4. Select "Authenticator App."
5. A **QR Code** will appear on your screen.
 - *If you are blind:* Use the "Enter code manually" option if available. It will give you a long string of letters/numbers.
 - *If you have sighted help:* Have them scan the QR code with your app.
6. Open your Authenticator App. Tap "+" to add an account.
 - Scan the QR code OR enter the manual code.
7. The app will now generate a 6-digit code that changes every 30 seconds.
8. Enter the current code from the app into the website to verify.
9. **SAVE YOUR BACKUP CODES.** The website will give you a list of one-time use codes. Print them or write them down. If you lose your phone, these are your only way back in.

Step 3: Repeat Do this for your Password Manager, Bank, and Social Media accounts.

Troubleshooting:

- If the code doesn't work, check your phone's time settings. 2FA codes rely on precise time synchronization. Enable "Set time automatically" in your phone settings.
-

CHAPTER 3: THIS MONTH (CUT THE TETHERS)

The Reality You've built your walls. Now you need to cut the tethers that bind you to the surveillance grid. Your phone number is a universal tracking ID used by data brokers to link your accounts, purchases, and locations into a single profile. Your cloud services (password managers, DNS) can be subpoenaed or breached. Your financial transactions are a permanent map of your life. You're still in the water—you're just swimming parallel to the shore. It's time to step onto the bank.

Do these five things this month:

1. **Get a burner number.** Hushed, AloSim, or Cape. Stop giving your real number to every app, form, and website that asks. Decouple your identity from your phone.
2. **Self-host what you can.** Bitwarden locally. NextDNS on your own terms. If you don't hold the data, someone else does.
3. **Compartmentalize.** Separate your identities. Work, personal, activism—different browsers, different emails, different numbers. One breach doesn't burn everything.
4. **Opt out of data brokers.** It's tedious. Do it anyway. Your address, relatives, and income are for sale right now. Delete what you can.
5. **The Payment Problem:** Cash is king for physical privacy, but the internet demands a trail. Credit cards are a permanent record. **Bitcoin is not the answer** — it's a public ledger, traceable by anyone. Use prepaid cards bought with cash for one-off purchases. For recurring needs, accept that a paper trail exists and minimize it. Use a dedicated email and burner number for these transactions. Don't confuse "convenience" with "privacy." If you can't pay without a trace, you aren't sovereign yet. You're just managing the leak.

Then organize someone. Host a kitchen-table session. Three people, one hour. Teach them what you just learned. You are now a node in a network. Act like one.

HOW-TO SHEET E:

HOW TO GET A BURNER NUMBER

Why? Your phone number is the key to your digital identity. It links your social media, banking, and shopping accounts. If you give it to a sketchy app, that app sells it to a broker, who sells it to a data aggregator, who sells it to a government agency. A burner number breaks this chain.

Option A: Hushed (App-based, Monthly)

1. Download the **Hushed** app from F-Droid (Android) or the App Store (iOS).
2. Create an account using your **burner email** (from Chapter 1).
3. Choose a number. You can pick a local area code or a toll-free number.
4. Pay using a prepaid card or gift card if possible to avoid linking your bank.
5. Use this number for all non-critical signups (shopping, newsletters, gym memberships).

Option B: AloSim (eSIM, USA)

1. Go to alosim.com.
2. Select a plan (e.g., 1GB for 7 days).
3. Purchase using a prepaid card or crypto (if available).
4. Scan the QR code to install the eSIM on your phone.
5. This gives you a temporary US number that you can discard after use.

Option C: Cape (VOIP, Privacy-focused)

1. Visit cape.com.
2. Sign up for a monthly plan.
3. Use this for more serious communication needs where you need a stable number but not your real one.

Important: Never use your burner number for critical accounts like your primary bank or government services. Keep those tied to your real identity (for now) but secured with a YubiKey.

HOW-TO SHEET F:

HOW TO OPT-OUT OF MAJOR DATA BROKERS

Why? Data brokers (like Whitepages, Spokeo, PeopleFinder) aggregate public records and sell them. They have your address, phone number, relatives, and estimated income. This data is used to build profiles for advertisers and, increasingly, for law enforcement without a warrant.

The Process:

1. **Identify the Brokers:** The major ones are:

- Whitepages
- Spokeo
- PeopleFinder
- BeenVerified
- Intelius
- FastPeopleSearch

2. **Manual Opt-Out (Free but Tedious):**

- Go to the broker's website.
- Search for your name and location.
- Click "Opt-Out" or "Remove My Info."
- You will often need to verify your identity (sometimes by sending a photo of your ID or a utility bill). **Be careful here.** If you don't want to send your ID, look for a "do not sell" link in their footer, though this is less effective.
- *Tip:* Create a dedicated email address for these requests so your main inbox isn't flooded.

3. **Automated Opt-Out (Paid but Easier):**

- Services like **DeleteMe** or **Incogni** will do this for you for a monthly fee. They scan hundreds of brokers and send removal requests automatically.
- *Trade-off:* You are trusting another company with your data to remove it from others. Only use this if you trust them implicitly.

Script for Verification Emails: *"I am requesting the immediate removal of my personal information from your database pursuant to my right to privacy. Please confirm when this has been completed."*

Note: This is a never-ending battle. New brokers appear, and old ones re-list your data. Do this quarterly.

HOW-TO SHEET G:

THE PAYMENT DILEMMA (MANAGING ONLINE TRANSACTIONS)

Why? Every credit card transaction creates a permanent record: Who you bought from, when, how much, and where you were. This data is sold to brokers and used to build a financial profile of your life.

The Reality: There is no perfect "anonymous online payment" that works for everyone yet.

- **Credit/Debit Cards:** Full trace. Avoid for sensitive purchases.
- **Bitcoin: NOT PRIVATE.** It is a public ledger. Anyone can trace your transaction history. Do not use it for privacy.
- **Monero (XMR):** Truly private cryptocurrency. Hard to acquire and spend. Only for advanced users.
- **Cash:** The only truly anonymous method. But you can't use it online.

The Strategy:

1. **Prepaid Cards:** Buy a Visa/Mastercard prepaid gift card with **cash** at a grocery store. Use this for online purchases. Do not register the card with your name.
2. **Dedicated Identities:** Create a separate email address and use a burner phone number for these transactions. Never link them to your real identity.
3. **Minimize the Trail:** If you must use a credit card, use a virtual card number (offered by some banks like Privacy.com) that limits spending and can be deleted instantly.
4. **Accept the Leak:** For essential recurring bills (internet, rent), you may have to use a card. Accept that this is a necessary leak. Focus your privacy efforts on the areas you *can* control.

Action:

- Go to a store. Buy a \$50 prepaid card with cash.
 - Create a new email: `yourname.shopping@tuta.com`
 - Use this combo for your next online purchase.
-

CHAPTER 4: THE HARD PART (GOING SOVEREIGN)

The Reality You have stopped the bleeding. You have built walls. You have cut the tethers. But you are still running on rented land.

You did not buy Windows. You did not buy macOS. You did not buy iOS. You licensed them. Microsoft, Apple, and Google own the code. They own the updates. They own the backdoors. They collect telemetry by default. They can brick your device, spy on your keystrokes, or force an update that breaks your workflow with a single click. You are a tenant in your own machine.

The Choice:

- **Stay Comfortable:** Keep using Windows/macOS/iOS. Accept that you are a product. Your data is the price of admission.
- **Go Sovereign:** Switch to **Linux** (Pop!_OS, Fedora, Debian) for your computer and **GrapheneOS** (on Pixel phones) for your mobile. These are open-source. The code is public. No hidden backdoors. No telemetry. You own the machine.

The Cost: It takes time to learn. Some apps won't work. It's inconvenient. You will have to troubleshoot.

The Reward: You are the administrator. No one else is watching. No one else is selling your data. You are free. You are *ACTUALLY* in charge.

Most people won't do this. That's fine. But if you want to be truly free, this is the only path.

Do these two things this month:

1. **Try Linux.** Don't wipe your drive yet. Boot from a Live USB. See if it works for you.
2. **Switch your phone.** If you have a Google Pixel, flash GrapheneOS. If not, strip your current phone with F-Droid and de-google it.

Then teach someone. Show a friend how to boot from a USB. Explain why "owning your code" matters. You are now a guardian of the open web.

HOW-TO SHEET H:

GETTING STARTED WITH LINUX

Why? Linux is the operating system of the internet. It is open-source, secure, and owned by no corporation. Pop!_OS is the best entry point for beginners because it looks familiar and works out of the box.

Step 1: Download Pop!_OS

1. Go to system76.com/pop.
2. Download the ISO file (choose the version for your computer architecture, usually "Intel/AMD").
3. Save it to your computer.

Step 2: Create a Live USB

1. Get a USB drive (at least 8GB). **Warning: This will erase everything on the USB drive.**
2. Download **BalenaEtcher** (balena.io/etcher) or **Ventoy**.
3. Open Etcher. Select the Pop!_OS ISO file. Select your USB drive. Click "Flash."
4. Wait for it to finish.

Step 3: Boot from USB (The "Try Before You Buy" Phase)

1. Plug the USB into your computer.
2. Restart your computer.
3. Immediately press the **Boot Menu key** (usually F12, F2, Esc, or Del depending on your manufacturer).
4. Select your USB drive from the list.
5. Choose **"Try this without installing."**
6. The computer will load Linux from the USB. You can browse the web, check email, and test your Wi-Fi.
Nothing is installed on your hard drive yet.

Step 4: Decide

- **If you like it:** Click the "Install" icon on the desktop. Follow the wizard. You can choose to "Erase Disk" (wipes Windows/Mac) or "Install alongside" (keeps your old OS).
- **If you don't like it:** Just restart and pull the USB out. Your old computer is unchanged.

Step 5: Basic Commands (For the Brave)

- Open the Terminal (Ctrl+Alt+T).
 - Update your system: `sudo apt update && sudo apt upgrade`
 - Install software: `sudo apt install firefox` (or use the "Pop!_Shop" graphical store).
-

HOW-TO SHEET I:

SWITCHING TO GRAPHENEOS (Andriod with privacy)

Why? Android with Google services is a surveillance device. It sends your location, contacts, and app usage to Google by default. **GrapheneOS** is a hardened, privacy-focused version of Android that removes Google entirely (unless you choose to add it back in a sandboxed way). It is the gold standard for mobile security.

Requirement: You **must** have a Google Pixel phone (Pixel 7 or newer recommended). Other phones do not have the necessary security hardware.

Step 1: Prepare Your Phone

1. Back up your data (photos, contacts) to a secure location (like a local drive or encrypted cloud).
2. Enable "Developer Options" in your phone settings (tap "Build Number" 7 times in "About Phone").
3. Enable "OEM Unlocking" and "USB Debugging" in Developer Options.

Step 2: Download the Installer

1. On your computer, go to grapheneos.org.
2. Download the **GrapheneOS Installer** (web-based tool is easiest).
3. Connect your phone to your computer via USB.

Step 3: Flash the OS

1. Open the installer in your browser.
2. Click "Unlock Bootloader." Your phone will reboot and warn you. Confirm. **This wipes your phone.**
3. Click "Install GrapheneOS." The installer will download the latest version and flash it to your phone.
4. Wait for the process to finish (10-20 minutes).
5. The phone will reboot into GrapheneOS.

Step 4: Initial Setup

1. Connect to Wi-Fi.
2. Set up your PIN/Pattern.
3. **Do not sign in to a Google Account.** You can add Google apps later in a "sandboxed" mode if you absolutely need them, but they will not have system-level access.
4. Install **F-Droid** (the open-source app store) from f-droid.org.
5. Install your privacy apps (Signal, Bitwarden, etc.) from F-Droid.

Verification: Go to grapheneos.org/faq#verifying-installation to verify the integrity of your installation.

Note: This process is technical. If you are not comfortable, watch a video tutorial first or ask a local Linux user group for help. But once it's done, your phone is yours again.

CHAPTER 5: THE LONG GAME (CHANGE THE RULES)

The Reality You've built your walls. You've cut your tethers. You've gone sovereign. You are safer than 99% of people on the internet.

It won't matter.

Individual privacy is a holding pattern, not a victory. The surveillance state doesn't need *you* specifically. It needs the herd. And as long as the herd is compliant, the system grows. Data brokers expand. Warrantless purchases increase. Laws weaken. Your encrypted drive doesn't protect your neighbor who just clicked "Accept All" and handed their life to a broker who sold it to an agency that couldn't be bothered with a warrant.

The waterfall is still there. You climbed out. Most people are still drifting.

The only way to dam the river is to change the rules.

Do these five things consistently:

1. **Track the legislation.** Look for bills in your country that ban warrantless government data purchases or regulate data brokers. Know who supports them. Know who opposes them.
2. **Contact your representatives.** Repeatedly. "I am a constituent. I want you to close the data broker loophole." One call is noise. Persistent calls are a signal. Silence is consent.
3. **Fund the fighters.** Support local and international NGOs (like EFF, Privacy International, or your country's equivalent) that are fighting in courtrooms and legislatures. Pay for the lawyers.
4. **Expose the abuse.** When surveillance overreach surfaces in your country, amplify it. Sunlight is the only disinfectant that works on secret programs.
5. **Vote like your data depends on it.** Because it does. Find out who supports privacy legislation. Show up for them. Campaign for them. Hold them accountable when they fold.

And never stop talking. Every conversation is a rope thrown to someone still in the water. Every person you educate is one fewer drifting toward the edge. Every person you organize is a brick in the dam.

HOW-TO SHEET K:

STARTING A LOCAL CHAPTER

Why? Online communities are powerful but fragile. They can be censored, infiltrated, or shut down. In-person networks survive outages, platform bans, and surveillance. A meetup in your city is infrastructure that can't be deleted.

Step 1: Find Your People

1. Start with your existing network. Friends, coworkers, family who are interested in privacy.
2. Post on local subreddits, Mastodon instances, or community boards: "Starting a privacy meetup in [City]. DM for details."
3. Reach out to local hacker spaces, Linux user groups, or EFF chapters. They already have the audience.
4. "Look for local chapters of **Privacy International**, **Electronic Frontier Foundation (EFF)**, or local digital rights groups like **Digital Rights Watch** (Australia) or **Open Rights Group** (UK)."

Step 2: Plan the First Meeting

1. **Venue:** A quiet café, a library meeting room, or someone's kitchen. Avoid corporate venues that require sign-ins.
2. **Size:** 3-5 people is enough. Don't wait for a crowd.
3. **Format:** One hour. 15 minutes for introductions. 30 minutes for a "teach" (pick one tool from this booklet and

demo it). 15 minutes for discussion and next steps.

4. **Ground Rules:** What happens at the meeting stays at the meeting. No recording. No photos. Respect everyone's threat model — some people are just curious, others are activists. Both belong.

Step 3: Establish Communication

1. Create a **Signal group** for the chapter. Not WhatsApp. Not Telegram. Signal.
2. Agree on a meeting cadence (monthly is good).
3. Rotate who leads the "*teach*" each session. This builds shared knowledge and prevents burnout.

Step 4: Take Action

1. Once the group is established, pick a local issue. Is your city deploying surveillance cameras? Is your school district monitoring students? Is a local data broker operating in your area? FLOCK "Safety" Cameras?
2. Organize a letter-writing night. Five people writing ten letters each = fifty letters to a representative.
3. Host a public workshop. Open it to newcomers. Grow the herd.
4. Research the specific privacy laws in your country. Is your government introducing new surveillance powers? Is there a local data broker operating? Focus your first campaign on a local or national issue that affects your specific community.

Safety Protocols:

- Never pressure anyone to share their real name or identity.
 - Never discuss illegal activity. This is about legal resistance.
 - If you suspect infiltration, tighten your circle and verify identities privately.
 - Trust is built slowly. Don't rush it.
-

HOW-TO SHEET J:

HOW TO CONTACT YOUR REPRESENTATIVES (GLOBAL GUIDE)

Why? Politicians in every country count calls and letters. If they hear nothing about privacy, they assume nobody cares. One call from you makes privacy a voting issue. Ten calls make it a priority. A hundred calls make it unavoidable.

Step 1: Find Your Representatives You need to identify the elected officials who represent your local area and the national legislature that writes the laws.

- **United States:**
 - **House of Representatives:** house.gov/representatives/find-your-representative
 - **Senate:** senate.gov/senators/senate-state-map
- **United Kingdom:**
 - **Members of Parliament (MPs):** parliament.uk/get-involved/contact-an-mp-or-lord
 - **Find your MP:** members.parliament.uk
- **European Union:**
 - **Members of the European Parliament (MEPs):** europarl.europa.eu/meps/en/home
 - **National Parliaments:** Search "[Your Country] parliament contact representatives".
- **Canada:**

- **Members of Parliament (MPs):** ourcommons.ca/members/en
- **Australia:**
 - **Members of Parliament:** aph.gov.au/Senators_and_Members
- **General Search:**
 - Search DuckDuckGo for: "find my representative [Your Country]" or "contact [Your Country] [Government Body]".
 - Look for official government domains (usually ending in .gov, .gc.ca, .parliament.uk, .eu, etc.).

Step 2: Make the Call

1. Call the office. A staffer will answer. Be polite and brief.
2. **Universal Script:**

"Hello, my name is [Your Name]. I am a constituent from [Your City/Town]. I am calling to ask [Representative's Name] to support legislation that closes the data broker loophole and bans warrantless government purchases of personal data. Privacy is a voting issue for me. Thank you."

3. The staffer will ask for your name and postal/zip code. Provide it. This confirms you are a constituent.
4. Thank them and hang up.

Step 3: Follow Up

1. Call again in two weeks. Same script.
2. Send an email. Same message.
3. Show up at a town hall or public forum. Ask the question publicly.

Tips:

- **Calls matter more than emails.** Letters matter more than calls. In-person matters most.
- **Be persistent but respectful.** Angry rants get dismissed. Polite repetition gets logged.
- **Encourage three friends to call.** Numbers are the currency of politics.
- **Adapt the Bill Name:** If your country doesn't have a "Fourth Amendment Act," look for the equivalent bill (e.g., "Data Protection Act," "Surveillance Reform Bill") and mention that specific name.

Last Thoughts

This is a decentralize movement. There is no "leader" to look up to or to assassinate. We are people who are sick of politicians and others who wish to take or privacy and freedoms away. This is your fight to win for yourself, your family and for others.

Pixelated Dwarf