Your Digital Surveillance First Aid Kit

(info is impact)

CREATED By @eymeikey

HEY!

2.

If you're reading this, you've used our zine generator and answered 3 questions about surveillance. THIS zine is your personal ~~starter~~ emergency kit.

It highlights the dangers of surveillance + + + gives you first tips to protect yourself from data access by 1312

TOPICS TOPICS TOPICS

- Location & movement 3
- Communication 4-5
- Online profiles & data 6-7
- Resources 8

No tool offers full protection – but this zine gives you a starting point to protect yourself and keep learning.

LET'S GO!

↑ NO COMPLETE GUIDE!

Module 1, Answer A

GPS, WLAN & Bluetooth

You thought Maps only shows you the way? Not just you. Your phone constantly sends signals:

GPS shows your exact location. Apps collect this data.

WLAN & Bluetooth send unique device IDs (e.g., when searching for networks) – even without connection.

How data is collected & used:

Sensors in public places capture these signals, track your movements, and create movement profiles. Authorities can, via court order locate all devices in an area at a specific time. They can also buy this data from Databrokers.

Protection Check:

KLACK

◆ Turn off location services & location history ◆ Revoke location access from apps - Activate airplane mode (prevents real-time tracking) ◆ Use an extra device BURNER PHONE

4.

Module 2: Block C

Content Scann[redacted]ng & Backdoors: When Your Messages Are Read

Private chats aren't always as private as they seem — even encrypted messages can be at risk.

Content Scanning (ChatControl)

Some politicians are pushing for messengers to scan your messages on your device before they're encrypted — aiming to detect certain content. This breaks the idea of end-to-end encryption, since messages must be readable before they can be protected.

Backdoors

These are intentionally built-in weaknesses in software or services that allow third parties (such as law enforcement or hackers) to access data without breaking the normal encryption. One example is how Meta could access WhatsApp metadata for years.

Protection Check:

5.

Use messengers with **true E2EE:** Choose services with default end-to-end encryption

Prefer **open source:** Pick messengers with open code (e.g. Signal, Element) — this allows independent security audits.

Share sensitive **info securely:** Only send private data via E2EE chats or trusted tools like ProtonMail (email) or Tresorit (cloud storage).

Stay informed: Follow political debates like the EU's "chat control" proposal, which threatens secure communication.

6.

Module 3: Block A

Trackers, Cook[redacted]es & F[redacted]ngerpr[redacted]nt[redacted]ng

Caught in the Act!
That ad wasn't random — it came from invisible tools tracking your online behavior: cookies, trackers, and fingerprinting.

What's happening:

Cookies store what sites you visit. Trackers follow you across websites. Fingerprinting identifies your device using unique traits like fonts, settings, or plugins — even without cookies. These tools build a profile of your interests. A quick search on AI surveillance can instantly tag you as "relevant."

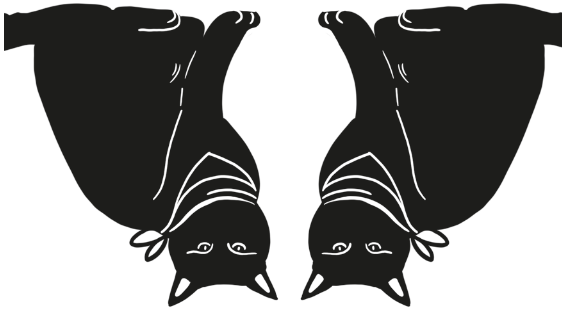
Law enforcement access:

Data brokers collect this info in bulk. Police and agencies can buy or request it to trace your activity or behavior.

Protection Check:

7.

- Use privacy-friendly browsers (e.g. Brave, Tor).
- Install blockers like uBlock Origin or Privacy Badger.
- Delete cookies regularly or limit them to sessions.
- Use a VPN to hide your IP. Switch to private search engines (DuckDuckGo, Startpage).



Resources:

8.

As you see Surveillance tech is everywhere – from AI analyzing messages to mass tracking in public. These tools keep evolving.

Digital security is a process. Staying informed and sharing what you learn helps everyone stay safer !!!

Check out these non-profit sources for updated cybersecurity info: