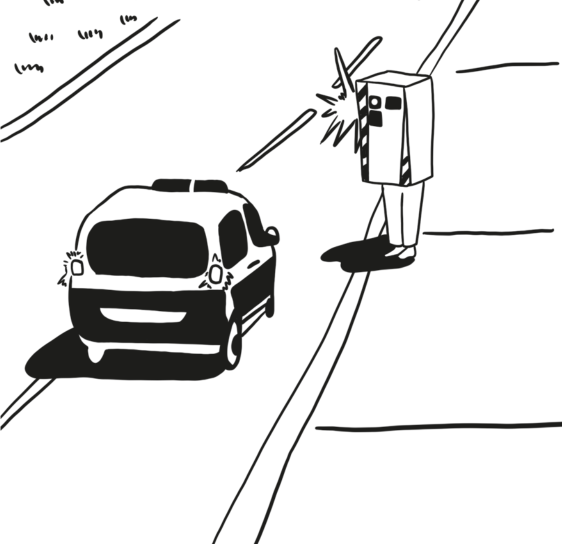
Your Digital Surveillance First Aid Kit

(catch the catchers)



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

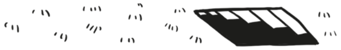
Content Scann[redacted]ng & Backdoors: When Your Messages Are Read

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.

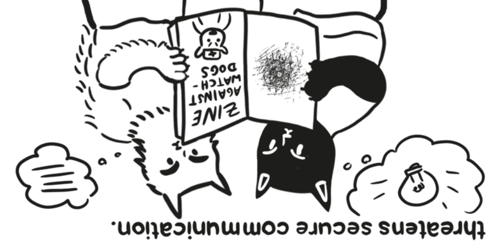
Protection Check: **5.**

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 B

Cloud Surve[redacted]llance & B[redacted]g Data

Many everyday services store massive amounts of your data in the cloud — a TREASURE for analysis algorithms.

What's happening:

Searches, emails, photos, documents, app use — everything is saved on cloud servers. AI-powered systems analyze this data to find patterns, predict your behavior, and build detailed profiles.

Targeted ads? That's the result: your interest in privacy triggered ads about "security."

Law enforcement access:

Authorities can access cloud data. The U.S. CLOUD Act allows access to U.S. companies' data even if stored abroad. Data can also be obtained via court orders or hacked accounts.

Protection Check: ✓✓✓✓ **7.**

- Use encrypted cloud services (e.g. Proton Drive, Tresorit)
- Upload only what's necessary
- Store sensitive files locally on encrypted drives
- Use strong passwords & 2FA Encrypt files (e.g. with VeraCrypt) before uploading

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:

CREATED BY @eymeikey