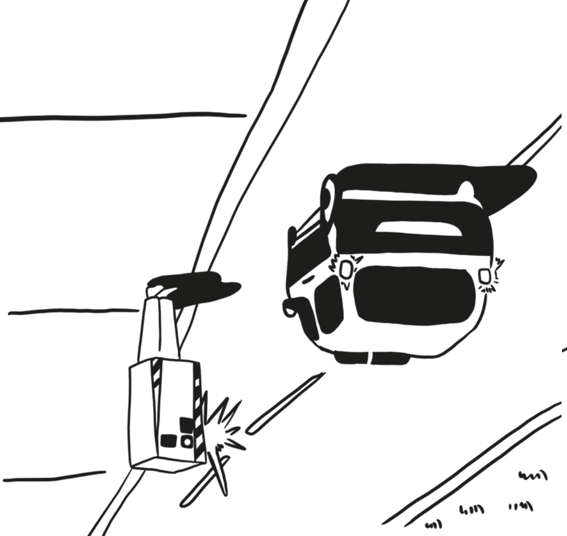
Your Digital Surveillance First Aid Kit

(catch the catchers)



HEY!

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

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 B:

Inv[redacted]s[redacted]ble Track[redacted]ng: Cell Towers & IMSI-Catchers

Even in your pocket, your phone connects to nearby towers. Your provider logs your location (cell data) – authorities can request this.

More intrusive:

An IMSI-Catcher pretends to be a real tower. Your phone connects and reveals:

- ◆ SIM ID (IMSI)
- ◆ location
- ◆ possibly SMS & calls (interceptable)

This often weakens encryption. IMSI-Catchers were used during the 2017 G20 protests in Hamburg. Note: This kind of surveillance often violates fundamental rights – but is still used by authorities.

Protection Check: Turn phone off (flight mode is not enough), use a burner phone, or store it in a Faraday pouch.

Module 2: Block A

Metadata - The Web of Connect[redacted]ons

You text your crush who's into abolition and data privacy – no reply. Maybe it's not what you wrote, but how it looked.

Even if messages are encrypted, metadata still reveals: Who talks to whom, when, how often, and from where. Like a sealed envelope: the content stays private, but everything on the outside is visible.

Authorities can use these traces to map out relationship networks – without ever reading a single message.

In Germany, access to metadata requires a court order. But providers often store it (due to data retention laws) and hand it over when asked.

COURTS ARE PART OF THE SYSTEM

Protection Check: ✓✓✓✓

Messenger:
Use Signal or Threema – collect minimal metadata + self-destructing messages.

Mail:

- ProtonMail / Tutanota – but remember: subject lines are also metadata.

Anonymous Browsing:

- VPN (ProtonVPN, Mullvad) hides your IP
- Tor Browser for max. anonymity
- Brave + DuckDuckGo = privacy-friendly

Data Safety:

- Clean photo metadata (e.g. ExifCleaner)
- Encrypt files before uploading (e.g. VeraCrypt)

Security Habits:

- Update devices regularly
- Strong passwords + 2FA
- Think about patterns: Reflect on what your digital behavior reveals.

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.

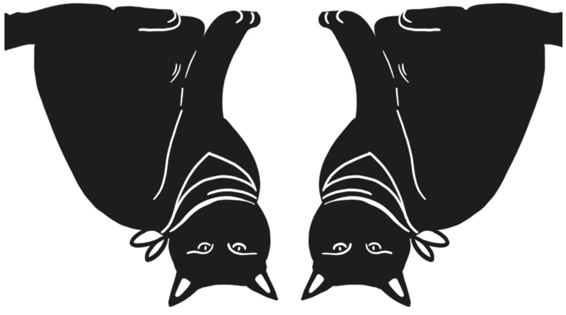
Protection Check:

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:

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