Your Digital Surveillance First Aid Kit
(info is impact)

LET'S GO!
(NO COMPLETE GUIDE!)

↓

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

TOPICS TOPICS TOPICS

- ⚡ Location & movement 1–3
- 💬 Communication 4–5
- 🖥 Online profiles & data 6–7
- 🔧 Resources 8

2.

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 🌀

GPS, WLAN & Bluetooth
Module 1, Answer A

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.

KLACK

Protection Check:

- ◆ 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 A
Metadata – The Web of Connections

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

5.
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.

---

6. Module 3: Block A
Trackers, Cookies & Fingerprinting

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.

7.
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).

8.
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:

[QR codes]