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

- 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.

NO COMPLETE GUIDE!

LET'S GO!

2.

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:

- 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

Protection Check: ✓✓✓✓ 5.

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 B

Cloud Surveillance & Big 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:

Your Digital Surveillance First Aid Kit

(info is impact)

CREATED By @eymeikey