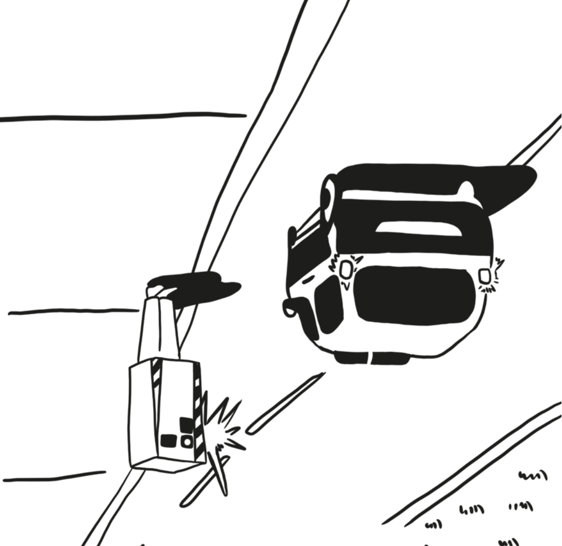
Your Digital Surveillance First Aid Kit

(catch the catchers)



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

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 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.

4. 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: ✓✓✓✓ **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)

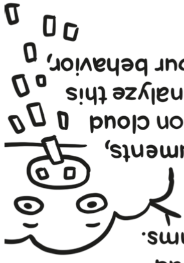
Security Habits:

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

6. Module 3: Block B

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

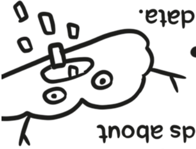
Many everyday services store massive amounts of your data in the cloud — a TREASURE for analysis algorithms.



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."

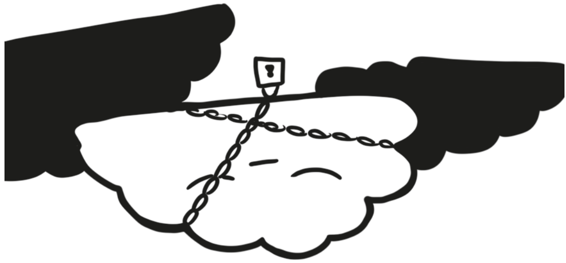


Law enforcement access:

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.**

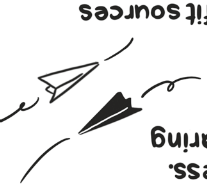
- Use encrypted cloud services (e.g. Proton Drive, Tresorit)
- Upload only what's necessary
- Store sensitive files locally on encrypted drives
- Use strong passwords & 2FA Encrypt files (e.g. with VeraCrypt) before uploading



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