

LET'S GO!

NO GUIDE! ↓

but this zine gives you a starting point to protect yourself and keep learning.

No tool offers full protection -

Resources

Location & movement 3
Communication 4-5
Online profiles & data 6-7

TOPICS TOPICS TOPICS

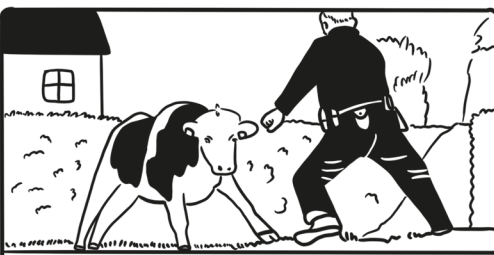
It highlights the dangers of surveillance + + gives you first tips to protect yourself from data access by 1312

If you're reading this, you've used our zine generator and answered 3 ques - your personal starter emergency kit.

HEY!

Your Digital Surveillance First Aid Kit

(break the fence not the spirit)



DISCLOSE.TV
K-9 Bites Cow, Deputy Tases K-9, Cow Kicks Deputy

The Digital Pen

Module 1, Answer C:

That shot of your fresh kicks? It may include hidden EXIF metadata — like GPS, time, camera, and phone model.

can use this:

From seized phones, unencrypted clouds, or via apps (e.g. WhatsApp) or data brokers. It can link you to places or protests.

Protection Check:

- Remove EXIF (e.g. ExifCleaner)
- Use Signal/Threema with DESTRUCTION MODE
- Avoid unencrypted cloud uploads
- Don't share , signs, or standout outfits
- Use strong passwords, 2FA & install updates

2.

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:



The Web of Connections

Module 2: Block A

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

4.

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).



7.

Metadata -

Module 3: Block A

Anonymous Browsing:

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

Quack

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.

Protection Check:

5.

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.

6.