

LET'S GO!

↓ NO GUIDE!

to protect yourself and keep learning.

but this zine gives you a starting point -

No tool offers full protection -

Resources 8

Online profiles & data 4-5

Communication 4-5

Location & movement 3

TOPICS TOPICS TOPICS TOPICS

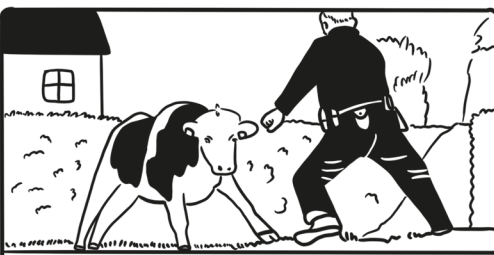
It highlights the dangers of surveillance + + gives you first tips to protect yourself from data access by 1312

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 standouts
- Use strong passwords, 2FA & install updates

Images & Metadata

4. Module 2: Block A

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

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:

- Share mindfully: Only share what feels necessary online.
- Adjust privacy settings: Check and update your settings on social media and apps.
- Keep identities separate: Use different emails or profiles for different activities.
- Be aware: Notice the digital footprints you leave.
- Check regularly: See what data companies have about you and manage it.



Protection Check:

5.

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 C

Your Online Profile

All your online activities — searches, social media, websites, purchases, and app use—are collected and combined into a detailed digital profile.

social media analysis

This profile reveals not only your interests but also preferences, political views, social networks, and even emotional states. The targeted ads you see show how precisely algorithms predict your needs and fears based on this data.

For law enforcement, such profiles are a treasure. They use them for open source intelligence (OSINT), predictive policing, and targeted surveillance to identify and monitor individuals.

