

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

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 -

tions about surveillance. This zine is your personal starter emergency kit.

HEY!

Your Digital Surveillance First Aid Kit

(for ppl who'd rather be cats :))



DON'T COMPARE US WITH DOGS WE DON'T WORK FOR THE POLICE

Module 1, Answer C: The Digital Cat

Images & Metadata


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/Therema with DESTRUCTION
- Encrypt files (e.g. with VeraCrypt)
- Avoid unencrypted cloud uploads
- Don't share , signs, or standouts outfits
- Use strong passwords, 2FA & install updates



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:



CREATED By @eymeikey

Module 2: Block C

When Your Messages Are Read

Private chats aren't always as private as they seem — even encrypted messages can be at risk.

Content Scanning (ChatControl)

Some politicians are pushing for messengers to scan your messages on your device before they're encrypted — aiming to detect certain content. This breaks the idea of end-to-end encryption, since messages must be readable before they can be protected.

Backdoors

These are intentionally built-in weaknesses in software or services that allow third parties (such as law enforcement or hackers) to access data without breaking the normal encryption. One example is how Meta could access WhatsApp metadata for years.

7.

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.



5.

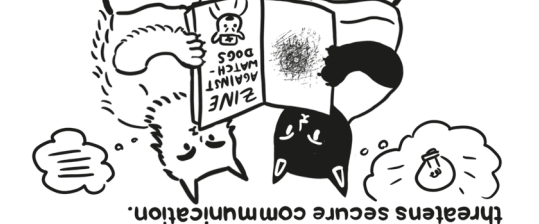
Protection Check:

Use messengers with **TRUE E2EE**: Choose services with default end-to-end encryption

Prefer open source: Pick messengers with open code (e.g. Signal, Element) — this allows independent security audits.

Share sensitive info securely. Only send private data via E2EE chats or trusted tools like ProtonMail (email) or Tresorit (cloud storage).

Stay informed: Follow political debates like the EU's "chat control" proposal, which threatens secure communication.



6. 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.

