

# LET'S GO!

NO COMPLETE GUIDE!

to protect yourself and keep learning.

but this zine gives you a starting point -

No tool offers full protection -

Resources

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

zine generator and answered 3 ques -

If you're reading this, you've used our

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 Footprint

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/TheBreema with DESTRUCTION MODE
- Encrypt files (e.g. with VeraCrypt)
- Avoid unencrypted cloud uploads
- Don't share QR signs, or standouts
- 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 B

### State Trojans & Spyware - The Invisible Threat

"Being watched before you even type 'Hi!'"

Sounds extreme — but it's real:

State trojans are programs secretly installed on your device by police or intelligence agencies to read everything — even before it's encrypted. They can access your microphone, camera, location, and passwords.

They often enter through security flaws in apps or operating systems.

Example: one WhatsApp bug let spyware install via a missed call.

In Germany, court orders are required, but critics warn that oversight is weak and courts often enable systemic abuse and unchecked state power.

Spyware from companies like NSO (Pegasus) has been used to target journalists, lawyers, and activists.

**Protection Check:**

- Keep software updated: Always update OS & apps to close security gaps.
- Beware of links/files: Don't click unknown links or open suspicious files.
- App permissions: Limit access to mic, camera, and location — only when needed.
- Strong passwords & 2FA: Protects accounts from being hijacked.
- Restart your device: May remove temporary infections.
- Sensitive conversations: Best offline or on a separate device.
- Tool check (if suspicious): Use Amnesty's Mobile Verification Toolkit (for tech-savvy users).
- Consult experts: If you suspect spyware or feel unsure, seek professional support.

## 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:

- Keep software updated: Always update OS & apps to close security gaps.
- Beware of links/files: Don't click unknown links or open suspicious files.
- App permissions: Limit access to mic, camera, and location — only when needed.
- Strong passwords & 2FA: Protects accounts from being hijacked.
- Restart your device: May remove temporary infections.
- Sensitive conversations: Best offline or on a separate device.
- Tool check (if suspicious): Use Amnesty's Mobile Verification Toolkit (for tech-savvy users).
- Consult experts: If you suspect spyware or feel unsure, seek professional support.

## 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.

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.