Your Digital Surveillance First Aid Kit

(info is impact)

CREATED BY @eymeikey

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

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 A

GPS, WLAN & Bluetooth

You thought Maps only shows you the way? Not just you. Your phone constantly sends signals:

GPS shows your exact location. Apps collect this data.

WLAN & Bluetooth send unique device IDs (e.g., when searching for networks) – even without connection.

How data is collected & used:

Sensors in public places capture these signals, track your movements, and create movement profiles. Authorities can, via court order locate all devices in an area at a specific time. They can also buy this data from Databrokers.

Protection Check:

KLACK

◆ Turn off location services & location history ◆ Revoke location access from apps - Activate airplane mode (prevents real-time tracking) ◆ Use an extra device

BURNER PHONE

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: ✓✓✓✓

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

Duuck

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 Onl[redacted]ne Prof[redacted]le

+ social media analysis

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.

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.

Resources:

As you see Surveillance tech is everywhere – from AI analyzing messages to mass tracking in public. These t◉◉ls 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: