Geospatial technologies + Digital security and privacy for counter-mappers

BN HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

Who am I?

Ben Hur Pintor

geospatial generalist. open stuff advocate. maptivist/datactivist.

Data Training Lead

Open Knowledge Foundation

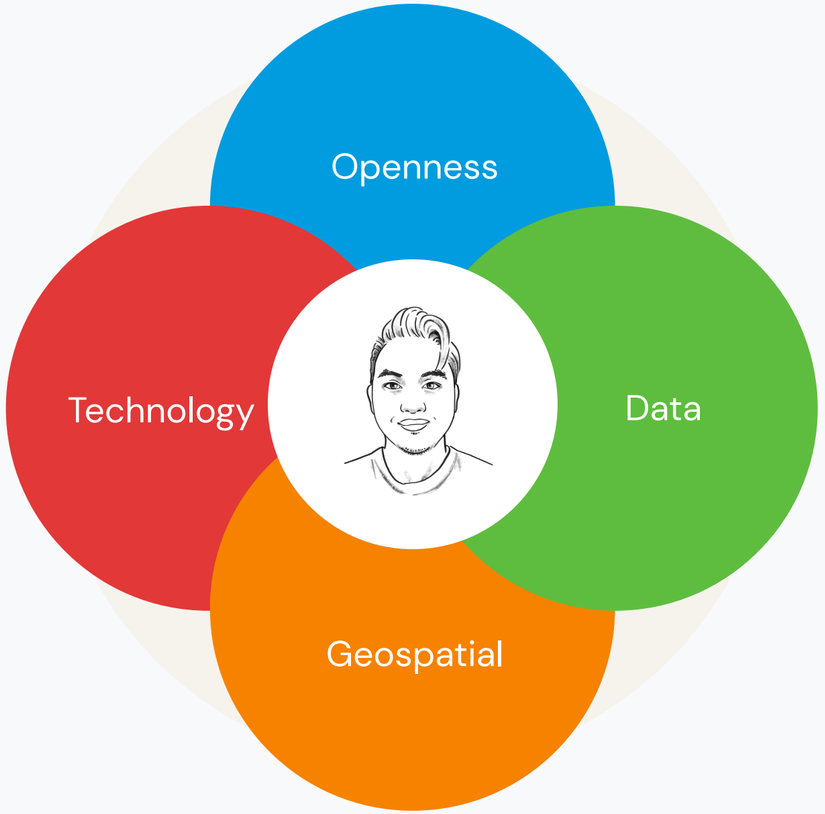
Proprietor

BN HR

openness.
data.
geospatial.

Chief Technology Officer

SmartCT
Citizens x Technology



Are these talks for me?

As a person who engages in counter-mapping—or similar activities such as advocacy work, defense of human rights, and social activism—it is important that you know technology can be used to:

1. **Advance your advocacy and improve the work that you do.**
2. **Protect yourself.**

I am not a cybersecurity expert or professional but I am a **practitioner and advocate of personal cybersecurity, digital privacy, and other digital rights** (e.g. right to repair, right to free and open knowledge).

Geospatial technologies for counter-mappers

BN HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

Counter-mapping appropriates technologies that were historically used to oppress and uses them to give power back to the people.

When you think about mapping, you think of...

- Geographic Information Systems (GIS)
- Remote Sensing (RS)
- High-resolution satellite imagery
- Precise positioning and geotagging applications (GPS)
- Surveys and census

Access to these technologies used to be limited to the State, large companies, and the elite.

Democratization
of technology

BN
HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

YOU GET A GIS
YOU GET A GIS
YOU GET A GIS
EVERYONE GETS A GIS
imgflip.com

- The Free Software Movement
- The Open Movement (open source, open hardware, open data, etc.)
- Higher price to performance ratio of computers
- Better technological literacy

All power to all the people.
POWER

Characteristics
of counter-mapping tools

A good counter-mapping tool is open, offline-friendly, and sustainable.

Open by default | Open by design

- **Accessible**
  - anyone can freely access and use it
- **Modifiable**
  - can easily be extended or modified according to need
- **Shareable**
  - can be shared among stakeholders without additional cost

Offline-friendly

- Usable even without access to the internet or cellular service such as in remote areas
- Offline-first tools and methodologies

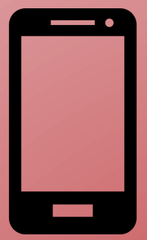
Sustainable

- Easy to set-up and maintain
- Minimal to no cost
- Causes minimum disruption to stakeholders
- Can run on old or refurbished hardware

Examples
of counter-mapping tools

GPS-enabled smartphone

- geotagging
- recording videos and audio
- note-taking
- communications



Data and survey collection tools

- Tools that allow you to collect data using your smartphone in remote and challenging environments.
  - ODK ODKX
  - KoBoToolbox
  - SABASI
- Sample guide: https://school-of-data.github.io/mobile-data-collection/

Drones and UAVs

- Commercial and hobby drones
- Collect imagery that is more up-to-date and with higher resolution than freely available satellite imagery
- Free flight planning applications

Processing UAV data (ODM)

- OpenDroneMap (https://www.opendronemap.org/)
- Open ecosystem for collecting, processing, analyzing and displaying aerial data with multiple applications and a growing community:
  - ODM
  - WebODM
  - NodeODM

Getting and sharing aerial imagery (OAM)

- OpenAerialMap (https://openaerialmap.org/)
- Open service to provide access to a commons of openly licensed imagery and map layer services
- OAM Browser (https://map.openaerialmap.org/)
  - provides a simple way to browse and obtain imagery

OpenAerialMap

Desktop GIS / geospatial applications

- QGIS (https://qgis.org)
- GRASS GIS (https://grass.osgeo.org/)
- PostGIS (https://postgis.net/)
- OSGeo (https://www.osgeo.org/) for a list of open source geospatial projects supported by the The Open Source Geospatial Foundation.

Web-mapping applications

- Leaflet (https://leafletjs.com/)
- MapLibre (https://maplibre.org/)
- Mapbox (https://www.mapbox.com/)

OpenStreetMap

- OpenStreetMap (https://www.openstreetmap.org/)
  - collaborative project to create a free editable map of the world

Maraming salamat!

BNHR

openness.
data.
geospatial.

@bnhr.xyz

@bnhrdotxyz

@bnhrdotxyz

bnhr.xyz

Digital security and privacy for counter-mappers

BN HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

I am not a cybersecurity expert or professional but I am a **practitioner and advocate of personal cybersecurity, digital privacy, and other digital rights** (e.g. right to repair, right to free and open knowledge).

This won’t be about enterprise or corporate cybersecurity but **more about individual security and privacy in the digital world**.

But I have nothing to hide, why should I care about privacy?

Privacy does not equal Secrecy

- We all know what happens in the bathroom but we still close the door.
- **Right to privacy** is an **inalienable right** be it in the physical or digital space.

Digital security and privacy at a glance

BN HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

#1

Digital privacy and security are shared responsibilities.

It takes a village...

- The State, the community, and your social circles play equally important roles in ensuring your digital security and privacy.
- Unfortunately, they will not always be your ally.

So what can you do?

- Be an **advocate**. **Inform and educate** those around you about digital security and try to convince them to be more secure online. Be patient with others.
- **Speak up and push back** against laws, rules, and regulations that erode our digital freedoms.
- **Support organizations** that seek to preserve and fight for our digital freedoms.

#2

You cannot protect yourself against everything all the time.

Know thy enemy/adversary

- It is **impractical** and **difficult** to protect all your data from everyone all the time.
- What's more important is for you to **understand the threats** you face and **how you can counter them** (**threat modeling**).

Threat models

A threat model is a list of the most probable threats to your security/privacy endeavors.

- An investigative journalist's threat model might be (protecting themselves against) the entities being investigated.
- A activist’s threat model might be (protecting themselves against) State surveillance.
- The average citizen's threat model might be (hiding their data from) large tech corporations.

Creating your threat model

Five questions:

1. **What** do I want to protect?
2. **Who** do I want to protect it from?
3. **How likely** is it that I will need to protect it?
4. **How bad** are the consequences if I fail?
5. **How much** trouble am I willing to go through to try to prevent potential consequences?

from: https://www.privacyguides.org/threat-modeling/#creating-your-threat-model

Example: Protecting your belongings

1. **What do I want to protect?**
    - Assets such as jewelry, electronics, important documents, or photos.
2. **Who do I want to protect it from?**
    - Adversaries such as burglars, roommates, or guests
3. **How likely is it that I will need to protect it?**
    - History of burglaries in the area? Trustworthiness of guests or roommates? How capable are your adversaries?
4. **How bad are the consequences if I fail?**
    - Is there anything you can't replace? Do you have insurance if something is stolen?
5. **How much trouble am I willing to go through to try to prevent potential** consequences?
    - Are you willing to buy a safe? Can you afford a CCTV system?

from: https://www.privacyguides.org/threat-modeling/#creating-your-threat-model

Simple Threat Modelling Exercise

GO TO THIS LINK: https://bit.ly/3mN45Iy

#3

There is no such thing as fully protected just better protected.

You can be compromised even w/o your fault

- Mass data breaches
- Data brokering
- People close to you being compromised
- Social engineering

Social engineering

The act of manipulating people into performing actions or divulging confidential information.

- Pop-culture examples: **Mr. Robot, Now You See Me, Catch Me If You Can**
- Recent real-world examples: **Apple and Meta shared data with hackers pretending to be law enforcement officials** (https://www.theverge.com/2022/3/30/23003600/apple-meta-shared-data-hackers-pretending-law-enforcement-officials)

Don’t let perfection be the enemy of the good

- Don’t get discouraged by the idea that you can’t ever be 100% protected, what’s more important is that you are taking steps to better protect yourself.

#4

Most of the time, more secure and private means less convenient.

Find the right balance for you

- Everything is a trade-off especially between security and convenience. Beware of the price you pay for your convenience.
- Some people quit before they even start because they become overwhelmed or want to do drastic changes. It’s okay to take it slow.

#5

Digital security and privacy is a personal journey.

The best way is the one that’s best for you

- You can tailor-fit your digital security strategy based on your own needs and capabilities.
- Threat modeling and understanding your threat models are important steps.
- Use the tools that work best for you.

#6

When in doubt, remember these two things: harden and compartmentalize.

Hardening

- Strengthening your security and privacy to avoid being compromised.
  - Using secure and privacy respecting tools and applications
  - Avoiding tools, applications, and situations that will compromise your privacy and security
  - Adding extra levels of security to your applications (e.g. encryption, 2FA, password manager)

Compartmentalization

- Make it harder for others to track or identify you online.
- Don’t put all your eggs in one basket—if one of your apps is compromised, you can minimize the damage to just that app.

Example:
two threats at three levels

Two threats at three levels

Two threat models:

1. Protecting your personal or private information from being compromised or hacked.
2. Avoid being tracked online or having your data collected without your consent (e.g. business surveillance, browser fingerprinting).

Three levels:

- Level 1 = Bare essentials. Easiest to achieve.
- Level 2 = More protection, more effort, a bit less convenient
- Level 3 = Most protection, most effort, possibly least convenient.

Passwords

Passwords: Level 1

- Do not reuse passwords.
- Use a password manager but do not use the one on your browser.
  - Cloud-based solutions like Lastpass or Bitwarden
- Lie on security questions.
- Use 2FA or 2-factor authentication.
- Avoid using your biometrics.

Passwords: Level 2

- Use hardware 2FA like YubiKey.

Passwords: Level 3

- Deploy your own password manager and host it on your own network.
  - Bitwarden is an open source password manager that you can deploy and host on your own.

Emails

Emails: Level 1

- Use privacy respecting email providers with end-to-end encryption especially for sensitive communications.
  - ProtonMail
  - Tutanota
- Use throwaway or disposable email addresses.
  - 10minutemail
  - Guerrilla Mail
  - ThrowAwayMail
  - EmailOnDeck

Emails: Level 2-3

- Use ONLY privacy-respecting email providers = delete your Google or Yahoo or other email accounts.

Messaging apps

Messaging apps

- Use privacy respecting instant messaging with end-to-end encryption especially for sensitive communications.
  - Signal (https://signal.org/en/)
  - Delta Chat (https://delta.chat/en/)
- Avoid using Facebook Messenger, Telegram, Viber, etc.

Digital Footprint

BN HR

liberty. data. geospatial.

@bnhr.xyz @bnhrdotxyz bnhrdotxyz https://bnhr.xyz

Digital Footprint: Level 1

- Disable Google tracking on your account.
- Disable tracking on your apps when not needed.
- Disconnect your email address from unused services / delete old accounts.
- Use random nicknames/usernames or fake information.

Digital Footprint: Level 2-3

- Delete your Google account (e.g. DeGoogle yourself)
- Compartmentalize your internet profiles/browsers.
- Use the Tor browser for social browsing.

Social Media

BN HR

liberty. data. geospatial.

@bnhr.xyz

@bnhrdotxyz

bnhrdotxyz

https://bnhr.xyz

Social Media: Level 1

- Minimize your use of the service.
- Utilize and enable all privacy settings.
- Disable notifications (for sanity).

Social Media: Level 2

- Lie. Do not put any private information on social media including photos of your face.
- Prefer using Progressive Web Apps (PWA) and web-app versions instead of the smartphone apps as these rarely track you actively.

Social Media: Level 3

- Delete your mainstream social media accounts.
- Use open source and decentralized alternatives.
  - PeerTube for YouTube
  - Mastodon for Twitter

Search engines

Search engines

- Stop using Google, Yahoo, or other search engines that track you.
- Use privacy respecting and non-tracking search engines.
  - Brave Search - uses its own index
  - Startpage - similar results to Google
  - DuckDuckGo - search history is saved in a non-identifiable manner
  - Searx - self-hostable, open source metasearch engine

Browsers

Browsers: Level 1

- Always delete your history or cache when accessing from public computers.
- Delete Google Chrome.
- Use more privacy-oriented browsers.
  - Brave
  - Safari
  - Firefox

Browsers: Level 2

- Harden Firefox.
- Compartmentalize browser use.
- Use the Tor browser for social browsing.

VPN

VPN (virtual private network)

- **NOTE: VPNs aren’t a security panacea.**
- In terms of security, the advantages of using a VPN include:
  - hiding your IP address
  - traffic/data is encrypted as it travels
- VPN providers: ProtonVPN, NordVPN, IVPN

Smartphones/mobile OS

Smartphone/Mobile OS: Level 1

- Disable tracking on your phone.
- Activate all privacy settings.
- Delete (if you can) all unwanted and unnecessary apps (e.g. bloatware).

Smartphone/Mobile OS: Level 2

- For Android users, use a custom ROM. The more privacy and security oriented, the better.
  - GrapheneOS
  - CalyxOS
  - /e/ OS
  - LineageOS
- Note that not all phones are supported by custom ROMs.

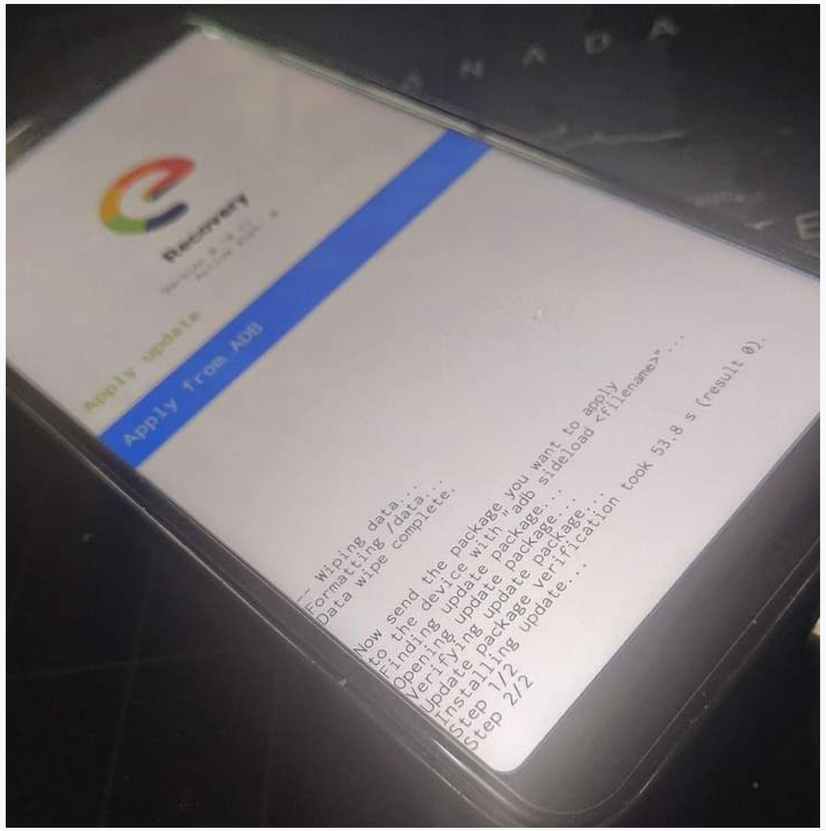
Smartphone/Mobile OS: Level 3

- Buy a privacy and security oriented phone.
  - Fairphone
  - Linux phones such as Librem and Pinephone
- Use a “dumb phone”.

Smartphone/Mobile OS

- Out of the box, **iOS is better** for privacy and security **than typical vendor-specific Android** (e.g. Samsung)
- **Stock** (e.g. Google Pixel) **or stockish** (e.g. Google One phones) **Android** will have **similar performance as iOS**.
- **Phones running custom Android ROMs or Linux** phones are **better than stock Android or iOS**.

Smartphone/Mobile OS



Apps on Custom Android ROMs

- **F-Droid** - hosts free and open source applications
- **Aurora Store, App Lounge, etc** - a Google PlayStore client/alternative that lets you install Android apps without the need for a Google account

Computers/Desktop OS

Oversimplified version

1 (least effective) to 3 (most effective)

Operating System	Privacy	Security	Anonymity
Windows	1	2	1
MacOS	2	2-3	2
Linux	2-3	2-3	2-3
Privacy-oriented Linux distribution (TailsOS, Whonix, Qubes)	3	3	3

It all depends on your threat model.

Personally, I’ve used Linux (in one distro or another) for almost 10 years and I haven’t had any problems/issues.

Payment

Payment

- Cash
- Privacy-based cryptocurrency like Monero
- Note: Non-private cryptocurrency like Bitcoin don’t have anonymous transactions. These transactions are all viewable on the blockchain which can be used to identify people if their wallet addresses are known.

Analog world

Payment

- Don’t use untrusted USB flash drives—see: bad USB, rubber ducky.
- Avoid putting personal information on public computers.
- Avoid using proprietary apps for fitness tracking or IOT devices.
- There are free and open source alternatives available.
- Cover your webcams or have a computer/laptop with hardware switches to disable the mic, camera, wifi, and bluetooth.
- HOST YOUR OWN STUFF. Build a home lab.

Other resources

- Privacy Guides: https://www.privacyguides.org/
- PrivacyTools.io: https://www.privacytools.io/
- Electronic Frontier Foundation: https://www.eff.org/

Maraming salamat!

BNHR

openness.
data.
geospatial.

@bnhr.xyz

@bnhrdotxyz

@bnhrdotxyz

bnhr.xyz

Except when expressly provided, this work and its contents by Ben Hur S. Pintor is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Other works (images, media, software, etc.) referenced in this work are under their own respective licenses.

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.