Hitchhiker’s Guide

A summary and action guide

Michael Obernhumer

24.4.2025

1 Introduction

This is a summarized checklist and to-do list aimed at increasing privacy and anonymity on the internet. It has been compiled based on the official Hitchhiker's Guide to Online Anonymity not including the links in the guide. Please note that this guide is **neither exhaustive nor guaranteed to be foolproof**. Its purpose is to provide a quick overview and actionable steps, **not** to replace the in-depth explanations and context found in the original guide. For comprehensive details, background information, and reasoning behind each recommendation, please refer to the full Hitchhiker's Guide. Keep in mind that none of these methods are foolproof, and each comes with potential trade-offs and risks.

2 Index

3 Your Network

3.1 Your IP address

Your IP address is easily accessible and can reveal identifying information about you. To protect your privacy, it's important to conceal or obfuscate your origin IP address — the one that can be linked directly to your identity. This can be achieved using one or a combination of the following methods:

- **Public Wi-Fi networks** (free)
- **The Tor anonymity network** (free)
- **VPN services used anonymously** (e.g., paid with cash or Monero)

3.2 Your DNS and IP Requests

By default, your DNS requests are handled by your Internet Service Provider (ISP), which logs them.

These requests are typically sent in plaintext, making them easy to intercept and monitor.

Recent studies have shown that **DNS over Tor** offers the most effective DNS privacy among available options. However, even this method can potentially be compromised through other techniques.

To further enhance your privacy and anonymity, consider the following approaches:

- **Tor Hidden DNS Services** or
- **ODoH (Oblivious DNS over HTTPS53)** — This method helps prevent a single intermediary from correlating the DNS query with your IP address. However, it is not effective against a **Global Passive Adversary (GPA)** who can monitor multiple parts of the communication chain simultaneously.
- **DoHoT (DNS over HTTPS over Tor)** — A newer method that routes encrypted DNS over the Tor network, offering enhanced anonymity. This approach requires some Linux expertise.

Other DNS privacy practices include:

- Using a **private DNS resolver** (e.g., Pi-hole, NextDNS, or DNS over Tor)
- Enabling **DoH (DNS over HTTPS)** or **DoT (DNS over TLS)**
- Using browsers that support **ECH (Encrypted Client Hello)** — currently, only Firefox-based browsers support ECH, and it must be enabled manually
- Ensuring your browser supports **OCSP (Online Certificate Status Protocol)** — this is enabled by default in most modern Firefox and Chromium-based browsers

It's also important to note that simple IP requests (e.g., loading a webpage) can still leak information about the site you're visiting, as many websites use unique IP addresses.

To address these concerns as thoroughly as possible, this guide will later recommend two primary solutions:

1. **Using Tor**
2. **Implementing a virtualized, multi-layered setup**, such as **VPN over Tor** (e.g., DNS over VPN over Tor or DNS over Tor)

3.3 Your RFID enabled devices

RFID in everyday items (cards, passport, phone, etc.) can be scanned without your knowledge, posing privacy risks like tracking or de-anonymization.

1. **Only carry RFID items when needed.**
2. **Use RFID-blocking wallets or pouches.**
3. **Be cautious in stores—some may scan all RFID tags.**
4. **Shield devices during sensitive activities (e.g. Farrady cage).**

3.4 The Wi-Fi and Bluetooth devices around you

Wi-Fi and Bluetooth signals are used to track your location and movements, even without GPS. Devices constantly scan nearby signals and send this data to companies like Google and Apple. This can be used for precise tracking—even through walls—by analyzing signal interference.

1. **Avoid carrying identifiable devices during sensitive activities.**
2. **For high privacy, stay in areas shielded like a Faraday cage.**
3. You could also try turning of Wi-F, Bluetooth, GPS,… but you cannot really trust these settings

3.5 Rogue Wi-Fi Access Points

Rogue Wi-Fi access points (APs) can trick your device into connecting to fake networks using de-auth attacks and spoofed portals. Once connected, attackers can monitor your traffic, steal credentials, and even bypass VPNs/Tor with advanced techniques.

1. **Avoid connecting to unknown/public Wi-Fi networks.**
2. **Always use a VPN/Tor (or VPN + Tor) on public networks.**
3. **Verify captive portals carefully, don't enter credentials unless you're sure it's legit.**

3.6 Traffic Anonymization

Tor and VPNs help protect your privacy, **but they're not invincible**. Advanced attacks like **correlation** and **timing analysis** can de-anonymize you by matching encrypted traffic patterns to known destinations or users — even **without decrypting anything**.

Common Attacks: - **Fingerprinting**: Match your encrypted Tor traffic to website patterns. - **Timing Attacks**: Correlate when you connect to Tor/VPN with when someone accesses a site. - **Counting Attacks**: Match download/upload sizes across networks.

Mitigations: - Don't access local services through anonymizers (e.g., don't Tor into your own university network). - Avoid heavily monitored networks (e.g., corporate or government). - Use **VPN over Tor** (or **Tor over VPN**) to add layers and confuse correlation attempts. - Use **public or residential Wi-Fi** for added unlinkability.

Important Notes: - Global surveillance adversaries (e.g., NSA) can still break anonymity with enough data. - Tor usage **alone** might flag you as suspicious in some contexts. - Tools like behavioral analysis or Wi-Fi/Bluetooth tracking can still deanonymize you indirectly.

For more, check out: - Attacks on Tor GitHub - Tor research survey - Tor 0day post

> Bottom line: Tor helps, but **don't rely on it alone** — especially against well-funded adversaries.

3.7 Some Devices can be tracked even when offline

Modern devices like:

- iPhones (iOS 13+)
- Samsung phones (Android 10+)
- MacBooks (macOS 10.15+)

can still broadcast Bluetooth signals even when turned off. Nearby online devices can pick this up, making offline tracking possible.

TL;DR: Don't bring these devices during sensitive activities or put them in a Farady pouch. "Off" doesn't mean invisible.

4 Your Hardware Identifiers

4.1 Your IMEI and IMSI

Every phone has two unique IDs:

- **IMEI** (device ID – tied to the hardware)
- **IMSI** (SIM ID – tied to your phone number and provider)

Whenever you connect to a mobile network, **both are logged** by operators and often shared with app makers, OS providers, and governments.

Why it matters: - Even **anonymous SIMs** can betray you if reused on a phone with a known IMEI. - **Antenna logs** can match your "burner" to your real phone based on signal strength and time. - **IMEI sale records** can trace the phone back to you—even if bought with cash, e.g. CCTV, Antenna logs. - **IMSI** is often tied to your ID (when SIMs require registration). - **Apple/Google** can track historical usage of your IMEI/IMSI. - **IMSI-catchers** (like Stingrays) can fake antennas to intercept calls, messages, or impersonate your number.

Best practices: - Use **burner phones** and **cash-bought SIMs** not tied to your identity. - Avoid reusing phones or SIMs. - Consider **anonymous online SIM services** that accept crypto (like Monero).

Note: Some "privacy" phones (e.g., Purism Librem) **still don't support IMEI randomization**, so full anonymity is tricky.

TL;DR: IMEI + IMSI = uniquely trackable. Use a truly separate device + SIM for sensitive actions.

4.2 Your Wi-Fi or Ethernet MAC address¶

Every device with Wi-Fi or Ethernet has a **MAC address** — a unique ID for your network hardware.

Why it's a privacy risk: - It can be **linked to the buyer** via manufacturer records (serial number + MAC). - Even cash-bought laptops may be traceable through **CCTV and antenna logs**. - OS vendors like **Apple, Google, Microsoft** log MACs for services like "Find My Device." - **Routers log MACs**, and many ISP-provided routers can be remotely accessed. - **Public/commercial networks** may track nearby MAC addresses (e.g., for traffic analysis).

Key point: If you used a device normally before using it for sensitive activity, it's likely already linked to you.

Protect yourself: - **Randomize your MAC address** — supported on Android, iOS, Linux, Windows 10/11. - **macOS does not support MAC randomization** — not ideal for privacy. - Avoid using your personal device for sensitive activities.

TL;DR: MAC addresses can silently link you to a device and place. Use MAC randomization or separate hardware.

4.3 Your Bluetooth MAC Address

Your **Bluetooth MAC** is another unique identifier — like your Wi-Fi MAC, but for Bluetooth.

Why it matters: - Manufacturers & OS vendors **log Bluetooth MACs**, potentially linking them to your identity or purchase. - Logs + billing info + **CCTV footage** + **antenna data** can be used to trace it back to you.

Privacy risks: - Can be used to **track your presence** in stores, public places, etc. - Some **vulnerabilities** still exist, even with protections.

What to do: - **Disable Bluetooth** entirely in BIOS/UEFI if possible — or via your OS if not. - On **Windows 10**, toggle the Bluetooth device in *Device Manager* to force address randomization.

TL;DR: Bluetooth tracking is less risky than Wi-Fi MAC tracking but still a concern. Disable it if not needed.

5 Your CPU

Modern **Intel** and **AMD CPUs** include hidden subsystems:

- **Intel Management Engine (IME)**
- **AMD Platform Security Processor (PSP)**

These can **run even when your PC is "off"**, have **network access**, and have had **serious vulnerabilities** in the past. Many consider IME a **backdoor**.

Privacy Tips: - Prefer **AMD CPUs** — fewer issues and no known remote backdoors. - **Disable IME/PSP** in BIOS (if possible). - Consider using **Coreboot/Libreboot** (if supported). - Use **virtual machines** for sensitive tasks. - Only use on **anonymous public networks**.

Check for vulnerabilities: - **Linux**: `spectre-meltdown-checker`
- **Windows**: InSpectre

6 OS and App Telemetry services

Most modern OSes — **Windows, macOS, Android, iOS, Ubuntu, Apps** — **collect telemetry by default**, even if you opt out. This data can include:

- Device identifiers
- App usage
- Location info

- Network activity

- Hardware/software details
- …

This data **can identify and track you**, even if anonymized.

What to Do: - Use **privacy-focused OSes** (e.g., Linux distros like Qubes). - Block telemetry via firewalls, host files, or tools (e.g., **O&O ShutUp10++** for Windows). - Minimize app installs; prefer **FOSS alternatives**. - Avoid smartphones for sensitive activity.

7 Your Smart Devices

Smartphones and smart devices constantly track:

- **Location, audio, habits, nearby devices**
- **Photos, accounts, networks**
- Data is often sent/stored **unencrypted**, even if you opt out.

Other culprits: smartwatches, speakers, fitness trackers, cars, tags.

Leave all smart devices behind for sensitive activities.

8 Yourself

8.1 Your Metadata

Metadata = info **about** your activity, not the content.
Think: *who* you contacted, *when*, *where* — not *what* was said.

Example:
You call an oncologist, then family — no one hears the call, but **the pattern speaks volumes**.

Metadata often includes: - Your **location** (from phones, OS, apps, websites)
- **Time and duration** of activity
- **Devices** involved
- Your **contacts** and their frequency

This data is: - Used in **geofencing warrants** (authorities request all devices at a place/time)
- **Sold** to militaries and third parties
- **Correlated** across ISPs, VPNs, platforms (even if each holds only part of the picture)

Even with a VPN: - The **VPN sees your traffic**, but not your ID
- The **ISP sees your ID**, but not your traffic
Together? They **could** trace you.

Minimize metadata leakage.
Use privacy tools + stay aware of what your devices reveal — even *without* your input.

8.2 Your Digital Footprint

Your **digital footprint** is more than just what you post or search — it's **how** you behave online. And that behavior is *shockingly unique*.

Behavior = Identity Even if you mask your IP, use a VPN, or disable cookies, systems can still identify you through:

- **Stylometry**: The way you write (word choice, grammar, punctuation, etc.)
- **Behavioral biometrics**: Typing speed, rhythm, mouse movements
- **Browser fingerprinting**: Fonts, extensions, screen size, OS, hardware
- **Keystroke logging**: Even if you don't submit a form
- **Cursor tracking & click behavior**: Your subconscious habits are identifiers

Even things like: > "You always click the same button first"
> "You use specific words or typos often"
…can be used to **link your identity** across platforms.

How to Minimize Fingerprinting

Tech helps, but behavior matters most.

1. **Use privacy-focused tools**:
    - Tor Browser (with JS disabled if needed)
    - Firefox with privacy extensions (like uBlock Origin, NoScript, CanvasBlocker)
    - Anti-fingerprinting OSes (like Tails or Qubes OS)
2. **Act differently with anonymous identities**:
    - Change typing habits (speed, spelling style)
    - Use different phrasing or vocabulary
    - Vary mouse/click behavior
    - Don't use your usual site/app flow or bookmarks

> You're playing a role. Don't leave behavioral breadcrumbs.

8.3 IRL and OSINT

Even with good privacy tools, sharing real-life details over time can expose you. This is where **OSINT (Open-Source Intelligence)** comes in—collecting public data like forum posts, photos, metadata, and social media to link identities.

Example: Hacker Jeremy Hammond was caught after casually mentioning personal facts online. Over time, those added up.

OSINT Resources: - OSINT Framework - Awesome OSINT GitHub - ReconTool

Stay Safe: - Don't reuse stories, habits, or writing styles - Avoid specific dates, places, or job info - Act like a completely different person online

You should never share real individual experiences/details using your anonymous identities that could later lead to finding your real identity.

> Every post is a puzzle piece. Don't let them add up.

8.4 Your Face, Voice, Biometrics and Pictures

Even if you're super careful, **your body can betray you**—especially your face.

Face Recognition Is Everywhere: - Platforms like **Facebook, Google, Snapchat** use it to tag and organize photos. - Even **random selfies in public** can capture your face and link you to a location and timestamp. - Uploaded images often include metadata (EXIF), and even without it, AI can estimate **when and where** the photo was taken.

Want to See This in Action? - Bellingcat's guides & videos show how **facial recognition** and **geolocation** are used in real investigations: - Facial Recognition in Investigations - Reverse Image Search Guide - Sun & Shadow Geolocation

Bottom Line: - **Avoid selfies** and **public appearances** if anonymity is critical. - Don't share photos or recordings tied to your voice, face, or body. - Remember, once your image is online, it's **almost impossible to take back**.