New Page

The Hitchhiker's Guide to Online Anonymity

(Or "How I learned to start worrying and love ~~privacy~~ anonymity")

Version 1.1.1, November 2021 by Anonymous Planet.

This guide is a work in progress. While I am doing the best I can to correct issues, inaccuracies, and improve the content, general structure, and readability; it will probably never be "finished".

There might be some wrong or outdated information in this guide because no human is omniscient, and humans do make mistakes. Please do not take this guide as a definitive gospel or truth because it is not. Mistakes have been written in the guide in earlier versions and fixed later when discovered. There are likely still some mistakes in this guide at this moment (hopefully few). Those are fixed as soon as possible when discovered.

Your experience may vary. Remember to check regularly for an updated version of this guide.

This guide is a non-profit open-source initiative, licensed under Creative Commons **Attribution-NonCommercial** 4.0 International ([cc-by-nc-4.0][] [[Archive.org]][27]).

- For mirrors see [Appendix A6: Mirrors]
- For help in comparing versions see [Appendix A7: Comparing versions]

Feel free to submit issues **(please do report anything wrong)** using GitHub Issues at:

https://github.com/AnonymousPlanet/thgtoa/issues

Feel free to come to discuss ideas at:

- GitHub Discussions: https://github.com/AnonymousPlanet/thgtoa/discussions
- Discord Server: https://discord.gg/V8dmd9y7mt
- Matrix/Element Room: `#anonymity:matrix.org` https://matrix.to/#/#anonymity:matrix.org

- Matrix Space: `#privacy-security-anonymity:matrix.org` https://matrix.to/#/#privacy-security-anonymity:matrix.org

Follow me on:

- Twitter at https://twitter.com/AnonyPla [[Nitter]][28] (cannot guarantee this account will stay up for long tho)
- Mastodon at https://mastodon.social/@anonypla.

To contact me, see the updated information on the website or send an e-mail to contact@anonymousplanet.org

Please consider [donating][Donations:] if you enjoy the project and want to support the hosting fees or support the funding of initiatives like the hosting of Tor Exit Nodes.

There are several ways you could read this guide:

- You want to understand the current state of online privacy and anonymity not necessarily get too technical about it: Just read the [Introduction][Introduction:], [Requirements][Pre-requisites and limitations:], [Understanding some basics of how some information can lead back to you and how to mitigate those][Understanding some basics of how some information can lead back to you and how to mitigate some:] and [A final editorial note][A small final editorial note:] sections.
- You want to do the above but also learn how to remove some online information about you: Just read the above and add the [Removing some traces of your identities on search engines and various platforms.][Removing some traces of your identities on search engines and various platforms:]
- You want to do the above and create online anonymous identities online safely and securely: Read the whole guide.

Precautions while reading this guide and accessing the various links:

- **Documents/Files** have a **[Archive.org]** link next to them for accessing content through Archive.org for increased privacy and in case the content goes missing. Some links are not yet archived or outdated on archive.org in which case I encourage you to ask for a new save if possible.
- **YouTube Videos** have a **[Invidious]** link next to them for accessing content through an Invidious Instance (in this case yewtu.be hosted in the Netherlands) for increased privacy. It is recommended to use these links when possible. See https://github.com/iv-org/invidious [[Archive.org]][29] for more information.
- **Twitter** links have a **[Nitter]** link next to them for accessing content through a Nitter Instance (in this case nitter.net) for increased privacy. It is recommended to use these links when possible. See https://github.com/zedeus/nitter [[Archive.org]][30] for more information.

- **Wikipedia** links have a **[Wikiless]** link next to them for accessing content through a Wikiless Instance (in this case Wikiless.org) for increased privacy. Again, it is recommended to use these links when possible. See https://codeberg.org/orenom/wikiless [[Archive.org]][31] for more information.
- If you are reading this in PDF or ODT format, you will notice plenty of ``` in place of double quotes (""). These ``` should be ignored and are just there to ease conversion into Markdown/HTML format for online viewing of code blocks on the website.

If you do not want the hassle and use one of the browsers below, you could also just install the following extension on your browser: https://github.com/SimonBrazell/privacy-redirect [[Archive.org]][32].

- Firefox: https://addons.mozilla.org/en-US/firefox/addon/privacy-redirect/
- Chromium-based browsers (Chrome, Brave, Edge): https://chrome.google.com/webstore/detail/privacy-redirect/pmcmeagblkinmogikoikkdjiligflglb

If you are having trouble accessing any of the many academic articles referenced in this guide due to paywalls, feel free to use Sci-Hub (https://en.wikipedia.org/wiki/Sci-Hub [[Wikiless]][33] [[Archive.org]][34]**) or LibGen (https://en.wikipedia.org/wiki/Library_Genesis** [[Wikiless]][35] [[Archive.org]][36]**) for finding and reading them. Because Science should be free. All of it.**

Finally note that this guide does mention and even recommends various commercial services (such as VPNs, CDNs, e-mail providers, hosting providers...) **but is not endorsed or sponsored by any of them in any way. There are no referral links and no commercial ties with any of these providers. This project is 100% non-profit and only relying on donations.**

Contents:

- [Pre-requisites and limitations:]
  - [Pre-requisites:]
  - [Limitations:]
- [Introduction:]
- [Understanding some basics of how some information can lead back to you and how to mitigate some:]
  - [Your Network:]
    - [Your IP address:]
    - [Your DNS and IP requests:]
    - [Your RFID enabled devices:]
    - [The Wi-Fi and Bluetooth devices around you:]

        - [Malicious/Rogue Wi-Fi Access Points:]
        - [Your Anonymized Tor/VPN traffic:]
        - [Some Devices can be tracked even when offline:]
    - [Your Hardware Identifiers:]
        - [Your IMEI and IMSI (and by extension, your phone number):]
        - [Your Wi-Fi or Ethernet MAC address:]
        - [Your Bluetooth MAC address:]
    - [Your CPU:]
    - [Your Operating Systems and Apps telemetry services:]
    - [Your Smart devices in general:]
    - [Yourself:]
        - [Your Metadata including your Geo-Location:]
        - [Your Digital Fingerprint, Footprint, and Online Behavior:]
        - [Your Clues about your Real Life and OSINT:]
        - [Your Face, Voice, Biometrics, and Pictures:]
        - [Phishing and Social Engineering:]
    - [Malware, exploits, and viruses:]
        - [Malware in your files/documents/e-mails:]
        - [Malware and Exploits in your apps and services:]
        - [Malicious USB devices:]
        - [Malware and backdoors in your Hardware Firmware and Operating System:]
    - [Your files, documents, pictures, and videos:]
        - [Properties and Metadata:]
        - [Watermarking:]
        - [Pixelized or Blurred Information:]
    - [Your Cryptocurrencies transactions:]
    - [Your Cloud backups/sync services:]
    - [Your Browser and Device Fingerprints:]
    - [Local Data Leaks and Forensics:]
    - [Bad Cryptography:]
    - [No logging but logging anyway policies:]
    - [Some Advanced targeted techniques:]
    - [Some bonus resources:]
    - [Notes:]
- [General Preparations:]
    - [Picking your route:]
        - [Timing limitations:]
        - [Budget/Material limitations:]
        - [Skills:]
        - [Adversarial considerations:]
    - [Steps for all routes:]
        - [Getting used to using better passwords:]
        - [Getting an anonymous Phone number:]
        - [Get a USB key:]
        - [Find some safe places with decent public Wi-Fi:]

- [The Tor Browser route:]
  - [Windows, Linux, and macOS:]
  - [Android:]
  - [iOS:]
  - [Important Warning:]
- [The Tails route:]
  - [Tor Browser settings on Tails:]
  - [Persistent Plausible Deniability using Whonix within Tails:]
- [Steps for all other routes:]
  - [Get a dedicated laptop for your sensitive activities:]
  - [Some laptop recommendations:]
  - [Bios/UEFI/Firmware Settings of your laptop:]
  - [Physically Tamper protect your laptop:]
- [The Whonix route:]
  - [Picking your Host OS (the OS installed on your laptop):]
  - [Linux Host OS:]
  - [macOS Host OS:]
  - [Windows Host OS:]
  - [Virtualbox on your Host OS:]
  - [Pick your connectivity method:]
  - [Getting an anonymous VPN/Proxy:]
  - [Whonix:]
  - [Tor over VPN:]
  - [Whonix Virtual Machines:]
  - [Pick your guest workstation Virtual Machine:]
  - [Linux Virtual Machine (Whonix or Linux):]
  - [Windows 10 Virtual Machine:]
  - [Android Virtual Machine:]
  - [macOS Virtual Machine:]
  - [KeepassXC:]
  - [VPN client installation (cash/Monero paid):]
  - [(Optional) Allowing only the VMs to access the internet while cutting off the Host OS to prevent any leak:]
  - [Final step:]
- [The Qubes Route:]
  - [Pick your connectivity method:][1]
  - [Getting an anonymous VPN/Proxy:][2]
  - [Note about Plausible Deniability:]
  - [Installation:]
  - [Lid Closure Behavior:]
  - [Connect to a Public Wi-Fi:]
  - [Updating Qubes OS:]
  - [Updating Whonix from version 15 to version 16:]
  - [Hardening Qubes OS:]
  - [Setup the VPN ProxyVM:]

        - [Setup a safe Browser within Qubes OS (optional but recommended):]
        - [Setup an Android VM:]
        - [KeePassXC:][3]
- [Creating your anonymous online identities:]
    - [Understanding the methods used to prevent anonymity and verify identity:]
        - [Captchas:]
        - [Phone verification:]
        - [E-Mail verification:]
        - [User details checking:]
        - [Proof of ID verification:]
        - [IP Filters:]
        - [Browser and Device Fingerprinting:]
        - [Human interaction:]
        - [User Moderation:]
        - [Behavioral Analysis:]
        - [Financial transactions:]
        - [Sign-in with some platform:]
        - [Live Face recognition and biometrics (again):]
        - [Manual reviews:]
    - [Getting Online:]
        - [Creating new identities:]
        - [Checking if your Tor Exit Node is terrible:]
        - [The Real-Name System:]
        - [About paid services:]
        - [Overview:]
        - [How to share files privately and/or chat anonymously:]
        - [How to share files publicly but anonymously:]
        - [Redacting Documents/Pictures/Videos/Audio safely:]
        - [Communicating sensitive information to various known organizations:]
        - [Maintenance tasks:]
- [Backing up your work securely:]
    - [Offline Backups:]
        - [Selected Files Backups:]
        - [Full Disk/System Backups:]
    - [Online Backups:]
        - [Files:]
        - [Information:]
    - [Synchronizing your files between devices Online:]
- [Covering your tracks:]
    - [Understanding HDD vs SSD:]
        - [Wear-Leveling.]
        - [Trim Operations:]
        - [Garbage Collection:]
        - [Conclusion:]
    - [How to securely wipe your whole Laptop/Drives if you want to erase everything:]

    - [Linux (all versions including Qubes OS):]
    - [Windows:]
    - [macOS:]
  - [How to securely delete specific files/folders/data on your HDD/SSD and Thumb drives:]
    - [Windows:][4]
    - [Linux (non-Qubes OS):]
    - [Linux (Qubes OS):]
    - [macOS:][5]
  - [Some additional measures against forensics:]
    - [Removing Metadata from Files/Documents/Pictures:]
    - [Tails:]
    - [Whonix:][6]
    - [macOS:][7]
    - [Linux (Qubes OS):][8]
    - [Linux (non-Qubes):]
    - [Windows:][9]
  - [Removing some traces of your identities on search engines and various platforms:]
    - [Google:]
    - [Bing:]
    - [DuckDuckGo:]
    - [Yandex:]
    - [Qwant:]
    - [Yahoo Search:]
    - [Baidu:]
    - [Wikipedia:]
    - [Archive.today:]
    - [Internet Archive:]
    - [Others:]
- [Some low-tech old-school tricks:]
  - [Hidden communications in plain sight:]
  - [How to spot if someone has been searching your stuff:]
- [Some last OPSEC thoughts:]
- [**If you think you got burned:**]
  - [If you have some time:]
  - [If you have no time:]
- [A small final editorial note:]
- [Donations:]
- [Helping others staying anonymous:]
- [Acknowledgments:]
- [Appendix A: Windows Installation]
  - [Installation:][10]
  - [Privacy Settings:]
- [Appendix B: Windows Additional Privacy Settings]
- [Appendix C: Windows Installation Media Creation]

- [Appendix D: Using System Rescue to securely wipe an SSD drive.]
- [Appendix E: Clonezilla]
- [Appendix F: Diskpart]
- [Appendix G: Safe Browser on the Host OS]
  - [If you can use Tor:]
  - [If you cannot use Tor:]
- [Appendix H: Windows Cleaning Tools]
- [Appendix I: Using ShredOS to securely wipe an HDD drive:]
  - [Windows:][11]
  - [Linux:]
- [Appendix J: Manufacturer tools for Wiping HDD and SSD drives:]
  - [Tools that provide a boot disk for wiping from boot:]
  - [Tools that provide only support from running OS (for external drives).]
- [Appendix K: Considerations for using external SSD drives]
  - [Windows:][12]
    - [Trim Support:]
    - [ATA/NVMe Operations (Secure Erase/Sanitize):]
  - [Linux:][13]
    - [Trim Support:][14]
    - [ATA/NVMe Operations (Secure Erase/Sanitize):][15]
  - [macOS:][16]
    - [Trim Support:][17]
    - [ATA/NVMe Operations (Secure Erase/Sanitize):][18]
- [Appendix L: Creating a mat2-web guest VM for removing metadata from files]
- [Appendix M: BIOS/UEFI options to wipe disks in various Brands]
- [Appendix N: Warning about smartphones and smart devices]
- [Appendix O: Getting an anonymous VPN/Proxy]
  - [Cash/Monero-Paid VPN:]
  - [Self-hosted VPN/Proxy on a Monero/Cash-paid VPS (for users more familiar with Linux):]
    - [VPN VPS:]
    - [Socks Proxy VPS:]
- [Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option]
- [Appendix Q: Using long-range Antenna to connect to Public Wi-Fis from a safe distance:]
- [Appendix R: Installing a VPN on your VM or Host OS.]
- [Appendix S: Check your network for surveillance/censorship using OONI]
- [Appendix T: Checking files for malware]
  - [Integrity (if available):]
  - [Authenticity (if available):]
  - [Security (checking for actual malware):]
    - [Anti-Virus Software:]
    - [Manual Reviews:][19]
- [Appendix U: How to bypass (some) local restrictions on supervised computers]
  - [Portable Apps:]

    - [Bootable Live Systems:]
    - [Precautions:]
- [Appendix V: What browser to use in your Guest VM/Disposable VM]
    - [Brave:]
    - [Ungoogled-Chromium:]
    - [Edge:]
    - [Safari:]
    - [Firefox:]
    - [Tor Browser:]
- [Appendix V1: Hardening your Browsers:]
    - [Brave:][20]
    - [Ungoogled-Chromium:][21]
    - [Edge:][22]
    - [Safari:][23]
    - [Firefox:][24]
        - [Normal settings:]
        - [Advanced settings:]
        - [Addons to install/consider:]
        - [Bonus resources:]
- [Appendix W: Virtualization]
- [Appendix X: Using Tor bridges in hostile environments]
- [Appendix Y: Installing and using desktop Tor Browser]
    - [Installation:][25]
    - [Usage and Precautions:]
- [Appendix Z: Online anonymous payments using cryptocurrencies]
    - [Reasonably anonymous option:]
    - [Extra-Paranoid anonymous option:]
    - [When using BTC: bonus step for improving your privacy using obfuscation:]
    - [When converting from BTC to Monero:]
- [Appendix A1: Recommended VPS hosting providers]
- [Appendix A2: Guidelines for passwords and passphrases]
- [Appendix A3: Search Engines]
- [Appendix A4: Counteracting Forensic Linguistics]
    - [Introduction:][26]
    - [What does an adversary look for when examining your writing?]
    - [Examples:]
    - [How to counteract the efforts of your adversary:]
    - [What different linguistic choices could say about you:]
        - [Emoticons:]
        - [Structural features:]
        - [Spelling slang and symbols:]
    - [Techniques to prevent writeprinting:]
        - [Spelling and grammar checking:]
        - [Translation technique:]
        - [Search and replace:]

    - [Final advice:]
  - [Bonus links:]
- [Appendix A5: Additional browser precautions with JavaScript enabled]
- [Appendix A6: Mirrors]
- [Appendix A7: Comparing versions]
- [Appendix A8: Crypto Swapping Services without Registration and KYC]
  - [General Crypto Swapping:]
  - [BTC to Monero only:]
- [Appendix A9: Installing a Zcash wallet:]
  - [Debian 11 VM:]
  - [Ubuntu 20.04 VM:]
  - [Windows 10 VM:]
  - [Whonix Workstation 16 VM:]
- [Appendix B1: Checklist of things to verify before sharing information:]
- [Appendix B2: Monero Disclaimer]
- [Appendix B3: Threat modeling resources]
- [References:]

Pre-requisites and limitations:

Pre-requisites:

- Understanding of the English language (in this case US English).
- Be a permanent resident in Germany where the courts have upheld up the legality of not using real names on online platforms (§13 VI of the German Telemedia Act of 2007[^1]'[^2]). **Alternatively, be a resident of any other country where you can confirm and verify the legality of this guide yourself.**
- This guide will assume you already have access to some (Windows/Linux/macOS) laptop computer (ideally not a work/shared device) and a basic understanding of how it works.
- Have patience as this process could take several weeks to complete if you want to go through all the content.
- Have some free time on your hands to dedicate to this process (or a lot depending on the route you pick).
- Be prepared to read a lot of references (do read them), guides (do not skip them), and follow a lot of how-to tutorials thoroughly (do not skip them either).
- Don't be evil (for real this time)[^3].

Limitations:

This guide is not intended for:

- Creating machine accounts of any kind (bots).
- Creating impersonation accounts of existing people (such as identity theft).
- Helping malicious actors conduct unethical, criminal, or illicit activities (such as trolling, stalking, disinformation, misinformation, harassment, bullying...).
- Use by minors.

Introduction:

TLDR for the whole guide: "A strange game. The only winning move is not to play" [^4]**.**

Making a social media account with a pseudonym or artist/brand name is easy. And it is enough in most use cases to protect your identity as the next George Orwell. There are plenty of people using pseudonyms all over Facebook/Instagram/Twitter/LinkedIn/TikTok/Snapchat/Reddit/... But the vast majority of those are anything but anonymous and can easily be traced to their real identity by your local police officers, random people within the OSINT[^5] (Open-Source Intelligence) community, and trolls[^6] on 4chan[^7].

This is a good thing as most criminals/trolls are not tech-savvy and will usually be identified with ease. But this is also a terrible thing as most political dissidents, human rights activists and whistleblowers can also be tracked rather easily.

This guide aims to provide an introduction to various de-anonymization techniques, tracking techniques, ID verification techniques, and optional guidance to creating and maintaining **reasonably and truly** online anonymous identities including social media accounts safely. This includes mainstream platforms and not only the privacy-friendly ones.

It is important to understand that the purpose of this guide is anonymity and not just privacy but much of the guidance you will find here will also help you improve your privacy and security even if you are not interested in anonymity. There is an important overlap in techniques and tools used for privacy, security, and anonymity but they differ at some point:

- **Privacy is about people knowing who you are but not knowing what you are doing.**
- **Anonymity is about people knowing what you are doing but not knowing who you are** [^8]**.**

![][37]

(Illustration from[^9])

Will this guide help you protect yourself from the NSA, the FSB, Mark Zuckerberg, or the Mossad if they are out to find you? Probably not ... Mossad will be doing "Mossad things" [^10] and will probably find you no matter how hard you try to hide[^11].

You must consider your threat model[^12] before going further.

![][38]

(Illustration by Randall Munroe, xkcd.com, licensed under CC BY-NC 2.5)

Will this guide help you protect your privacy from OSINT researchers like Bellingcat[^13], Doxing[^14] trolls on 4chan[^15], and others that have no access to the NSA toolbox? More likely. Tho I would not be so sure about 4chan.

Here is a basic simplified threat model for this guide:

![][39]

(Note that the "magical amulets/submarine/fake your own death" jokes are quoted from the excellent article "This World of Ours" by James Mickens, 2014above[^10])

Disclaimer: Jokes aside (magical amulet...). Of course, there are also advanced ways to mitigate attacks against such advanced and skilled adversaries but those are just out of the scope of this guide. It is crucially important that you understand the limits of the threat model of this guide. And therefore, this guide will not double in size to help with those advanced mitigations as this is just too complex and will require an exceedingly high knowledge and skill level that is not expected from the targeted audience of this guide.

The EFF provides a few security scenarios of what you should consider depending on your activity. While some of those tips might not be within the scope of this guide (more about Privacy than Anonymity), they are still worth reading as examples. See https://ssd.eff.org/en/module-categories/security-scenarios [[Archive.org]][40].

If you want to go deeper into threat modeling, see [Appendix B3: Threat modeling resources].

You might think this guide has no legitimate use but there are many[^16]'[^17]'[^18]'[^19]'[^20]'[^21]'[^22] such as:

- Evading Online Censorship[^23]
- Evading Online Oppression
- Evading Online Stalking, Doxxing, and Harassment
- Evading Online Unlawful Government Surveillance
- Anonymous Online Whistle Blowing
- Anonymous Online Activism

- Anonymous Online Journalism
- Anonymous Online Legal Practice
- Anonymous Online Academic Activities (For instance accessing scientific research where such resources are blocked). See note below.
- ...

This guide is written with hope for those **good-intended individuals** who might not be knowledgeable enough to consider the big picture of online anonymity and privacy.

Lastly, use it at your own risk. Anything in here is not legal advice and you should verify compliance with your local law before use (IANAL[^24]**). "Trust but verify"**[^25] **all the information yourself (or even better, "Never Trust, always verify"**[^389]**). I strongly encourage you to inform yourself and do not hesitate to check any information in this guide with outside sources in case of doubt. Please do report any mistake you spot to me as I welcome criticism. Even harsh but sound criticism is welcome and will result in having the necessary corrections made as quickly as possible.**

Understanding some basics of how some information can lead back to you and how to mitigate some:

There are many ways you can be tracked besides browser cookies and ads, your e-mail, and your phone number. And if you think only the Mossad or the NSA/FSB can find you, you would be wrong.

First, you could also consider these more general resources on privacy and security to learn more basics:

- The New Oil: https://thenewoil.org/ [[Archive.org]][41]
- Techlore videos: https://www.youtube.com/c/Techlore [[Invidious]][42]
- Privacy Guides: https://privacyguides.org/ [[Archive.org]][43]

If you skipped those, you should really still consider viewing this YouTube playlist from the Techlore Go Incognito project (https://github.com/techlore-official/go-incognito [[Archive.org]][44]) as an introduction before going further:

https://www.youtube.com/playlist?list=PL3KeV6Ui_4CayDGHw64OFXEPHgXLkrtJO [[Invidious]][45]. This guide will cover many of the topics in the videos of this playlist with more details and references as well as some added topics not covered within that series. This will just take you 2 or 3 hours to watch it all.

Now, here is a non-exhaustive list of some of the many ways you could be tracked and de-anonymized:

Your Network:

Your IP address:

Disclaimer: this whole paragraph is about your public-facing Internet IP and not your local network IP.

Your IP address[^26] is the most known and obvious way you can be tracked. That IP is the IP you are using at the source. This is where you connect to the internet. That IP is usually provided by your ISP (Internet Service Provider) (xDSL, Mobile, Cable, Fiber, Cafe, Bar, Friend, Neighbor). Most countries have data retention regulations[^27] that mandate keeping logs of who is using what IP at a certain time/date for up to several years or indefinitely. Your ISP can tell a third party that you were using a specific IP at a specific date and time, years after the fact. If that IP (the original one) leaks at any point for any reason, it can be used to track down you directly. In many countries, you will not be able to have internet access without providing some form of identification to the provider (address, ID, real name, e-mail ...).

Needless to say, that most platforms (such as social networks) will also keep (sometimes indefinitely) the IP addresses you used to sign-up and sign into their services.

Here are some online resources you can use to find some information about your current **public IP** right now:

- Find your IP:
  - https://resolve.rs/
  - https://www.dnsleaktest.com/ (Bonus, check your IP for DNS leaks)
- Find your IP location or the location of any IP:
  - https://resolve.rs/ip/geolocation.html
- Find if an IP is "suspicious" (in blocklists) or has downloaded "things" on some public resources:
  - https://mxtoolbox.com/blacklists.aspx
  - https://www.virustotal.com/gui/home/search

    - https://iknowwhatyoudownload.com (Take this with a grain of salt, it might not show anything interesting and has limited data sources. This is more for fun than anything serious.)
- Registration information of an IP (most likely your ISP or the ISP of your connection who most likely know who is using that IP at any time):
    - https://whois.domaintools.com/
- Check for open-services or open devices on an IP (especially if there are leaky Smart Devices on it):
    - https://www.shodan.io/host/185.220.101.134 (replace the IP by your IP or any other, or change in the search box, this example IP is a Tor Exit node)
- Various tools to check your IP such as block-lists checkers and more:
    - https://browserleaks.com/ip
    - https://www.whatismyip.com
- Would you like to know if you are connected through Tor?
    - https://check.torproject.org

For those reasons, we will need to obfuscate and hide that origin IP (the one tied to your identification) or hide it as much as we can through a combination of various means:

- Using a public Wi-Fi service (free).
- Using the Tor Anonymity Network[^28] (free).
- Using VPN[^29] services anonymously (anonymously paid with cash or Monero).

Do note that, unfortunately, these solutions are not perfect, and you will experience performance issues[^30].

All those will be explained later in this guide.

Your DNS and IP requests:

DNS stands for "Domain Name System"[^31] and is a service used by your browser (and other apps) to find the IP addresses of a service. It is a huge "contact list" (phone book for older people) that works like asking it a name and it returns the number to call. Except it returns an IP instead.

Every time your browser wants to access a certain service such as Google through www.google.com. Your Browser (Chrome or Firefox) will query a DNS service to find the IP addresses of the Google web servers.

Here is a video explaining DNS visually if you are already lost:

https://www.youtube.com/watch?v=vrxwXXytEuI [[Invidious]][46]

Usually, the DNS service is provided by your ISP and automatically configured by the network you are connecting to. This DNS service could also be subject to data retention regulations or will just

keep logs for other reasons (data collection for advertising purposes for instance). Therefore, this ISP will be capable of telling everything you did online just by looking at those logs which can, in turn, be provided to an adversary. Conveniently this is also the easiest way for many adversaries to apply censoring or parental control by using DNS blocking[^32]. The provided DNS servers will give you a different address (than their real one) for some websites (like redirecting thepiratebay.org to some government website). Such blocking is widely applied worldwide for certain sites[^33].

Using a private DNS service or your own DNS service would mitigate these issues, but the other problem is that most of those DNS requests are by default still sent in clear text (unencrypted) over the network. Even if you browse PornHub in an incognito Window, using HTTPS and using a private DNS service, chances are exceedingly high that your browser will send a clear text unencrypted DNS request to some DNS servers asking basically "So what's the IP address of www.pornhub.com?".

Because it is not encrypted, your ISP and/or any other adversary could still intercept (using a Man-in-the-middle attack[^96]) your request will know and possibly log what your IP was looking for. The same ISP can also tamper with the DNS responses even if you are using a private DNS. Rendering the use of a private DNS service useless.

As a bonus, many devices and apps will use hardcoded DNS servers bypassing any system setting you could set. This is for example the case with most (70%) Smart TVs and a large part (46%) of Game Consoles[^34]. For these devices, you will have to force them[^35] to stop using their hardcoded DNS service which could make them stop working properly.

A solution to this is to use encrypted DNS using DoH (DNS over HTTPS[^36]), DoT (DNS over TLS[^37]) with a private DNS server (this can be self-hosted locally with a solution like pi-hole[^38], remotely hosted with a solution like nextdns.io or using the solutions provider by your VPN provider or the Tor network). This should prevent your ISP or some go-between from snooping on your requests ... except it might not.

Small in-between Disclaimer: **This guide does not necessarily endorse or recommends Cloudflare services even if it is mentioned several times in this section for technical understanding.**

Unfortunately, the TLS protocol used in most HTTPS connections in most Browsers (Chrome/Brave among them) will leak the Domain Name again through SNI[^39] handshakes (this can be checked here at Cloudflare: https://www.cloudflare.com/ssl/encrypted-sni/ [[Archive.org]][47]). **As of the writing of this guide, only Firefox-based browsers supports ECH (Encrypted Client Hello** [^40] **previously known as eSNI**[^41]**) on some websites which will encrypt everything end to end (in addition to using a secure private DNS over TLS/HTTPS) and will allow you to hide your DNS requests from a third party**[^42]**.** And this option is not enabled by default either so you will have to enable it yourself.

![][48]

In addition to limited browser support, only Web Services and CDNs[^43] behind Cloudflare CDN support ECH/eSNI at this stage[^44]. This means that ECH and eSNI are not supported (as of the writing of this guide) by most mainstream platforms such as:

- Amazon (including AWS, Twitch...)
- Microsoft (including Azure, OneDrive, Outlook, Office 365...)
- Google (including Gmail, Google Cloud...)
- Apple (including iCloud, iMessage...)
- Reddit
- YouTube
- Facebook
- Instagram
- Twitter
- GitHub
- ...

Some countries like Russia[^45] and China[^46] might (unverified despite the articles) block ECH/eSNI handshakes at the network level to allow snooping and prevent bypassing censorship. Meaning you will not be able to establish an HTTPS connection with a service if you do not allow them to see what it was.

The issues do not end here. Part of the HTTPS TLS validation is called OCSP[^47] and this protocol used by Firefox-based browsers will leak metadata in the form of the serial number of the certificate of the website you are visiting. An adversary can then easily find which website you are visiting by matching the certificate number[^48]. This issue can be mitigated by using OCSP stapling[^49]. Unfortunately, this is enabled but not enforced by default in Firefox/Tor Browser. But the website you are visiting must also be supporting it and not all do. Chromium-based browsers on the other hand use a different system called CRLSets[^50]'[^51] which is arguably better.

Here is a list of how various browsers behave with OCSP: https://www.ssl.com/blogs/how-do-browsers-handle-revoked-ssl-tls-certificates/ [[Archive.org]][49]

Here is an illustration of the issue you could encounter on Firefox-based browsers:

![][50]

Finally, even if you use a custom encrypted DNS server (DoH or DoT) with ECH/eSNI support and OCSP stapling, it might still not be enough as traffic analysis studies[^52] have shown it is still possible to reliably fingerprint and block unwanted requests. Only DNS over Tor was able to show efficient DNS Privacy in recent studies but even that can still be defeated by other means (see [Your Anonymized Tor/VPN traffic][Your Anonymized Tor/VPN traffic:]).

One could also decide to use a Tor Hidden DNS Service or ODoH (Oblivious DNS over HTTPS[^53]) to further increase privacy/anonymity but **unfortunately**, as far as I know, these methods are only provided by Cloudflare as of this writing (https://blog.cloudflare.com/welcome-hidden-resolver/ [[Archive.org]][51],

https://blog.cloudflare.com/oblivious-dns/ [[Archive.org]][52]). These are workable and reasonably secure technical options but there is also a moral choice if you want to use Cloudflare or not (despite the risk posed by some researchers[^54]).

Lastly, there is also this new possibility called DoHoT which stands for DNS over HTTPS over Tor which could also further increase your privacy/anonymity and which you could consider if you are more skilled with Linux. See https://github.com/alecmuffett/dohot [[Archive.org]][53]. This guide will not help you with this one at this stage, but it might be coming soon.

Here is an illustration showing the current state of DNS and HTTPS privacy based on my current knowledge.

![][54]

As for your normal daily use (non-sensitive), remember that only Firefox-based browsers support ECH (formerly eSNI) so far and that it is only useful with websites hosted behind Cloudflare CDN at this stage. If you prefer a Chrome-based version (which is understandable for some due to some better-integrated features like on-the-fly Translation), then I would recommend the use of Brave instead which supports all Chrome extensions and offers much better privacy than Chrome.

But the story does not stop there right. Now because after all this, even if you encrypt your DNS and use all possible mitigations. Simple IP requests to any server will probably allow an adversary to still detect which site you are visiting. And this is simply because the majority of websites have unique IPs tied to them as explained here: https://blog.apnic.net/2019/08/23/what-can-you-learn-from-an-ip-address/ [[Archive.org]][55]. This means that an adversary can create a dataset of known websites for instance including their IPs and then match this dataset against the IP you ask for. In most cases, this will result in a correct guess of the website you are visiting. This means that despite OCSP stapling, despite ECH/eSNI, despite using Encrypted DNS ... An adversary can still guess the website you are visiting anyway.

Therefore, to mitigate all these issues (as much as possible and as best as we can), this guide will later recommend two solutions: Using Tor and a virtualized (See [Appendix W: Virtualization][Appendix V1: Hardening your Browsers:]) multi-layered solution of VPN over Tor solution (DNS over VPN over Tor or DNS over TOR). Other options will also be explained (Tor over VPN, VPN only, No Tor/VPN) but are less recommended.

Your RFID enabled devices:

RFID stands for Radio-frequency identification[^55], it is the technology used for instance for contactless payments and various identification systems. Of course, your smartphone is among those devices and has RFID contactless payment capabilities through NFC[^56]. As with everything else, such capabilities can be used for tracking by various actors.

But unfortunately, this is not limited to your smartphone, and you also probably carry some amount of RFID enabled device with you all the time such as:

- Your contactless-enabled credit/debit cards
- Your store loyalty cards
- Your transportation payment cards
- Your work-related access cards
- Your car keys
- Your national ID or driver license
- Your passport
- The price/anti-theft tags on object/clothing
- ...

While all these cannot be used to de-anonymize you from a remote online adversary, they can be used to narrow down a search if your approximate location at a certain time is known. For instance, you cannot rule out that some stores will effectively scan (and log) all RFID chips passing through the door. They might be looking for their loyalty cards but are also logging others along the way. Such RFID tags could be traced to your identity and allow for de-anonymization.

More information over at Wikipedia: https://en.wikipedia.org/wiki/Radio-frequency_identification#Security_concerns [[Wikiless]][56] [[Archive.org]][57] and https://en.wikipedia.org/wiki/Radio-frequency_identification#Privacy [[Wikiless]][56] [[Archive.org]][57]

The only way to mitigate this problem is to have no RFID tags on you or to shield them again using a type of Faraday cage. You could also use specialized wallets/pouches that specifically block RFID communications. Many of those are now made by well-known brands such as Samsonite[^57]. You should just not carry such RFID devices while conducting sensitive activities.

See [Appendix N: Warning about smartphones and smart devices]

The Wi-Fi and Bluetooth devices around you:

Geolocation is not only done by using mobile antennas triangulation. It is also done using the Wi-Fi and Bluetooth devices around you. Operating systems makers like Google (Android[^58]) and Apple (IOS[^59]) maintain a convenient database of most Wi-Fi access points, Bluetooth devices, and their location. When your Android smartphone or iPhone is on (and not in Plane mode), it will scan actively (unless you specifically disable this feature in the settings) Wi-Fi access points, and Bluetooth devices around you and will be able to geolocate you with more precision than when using a GPS.

This active and continuous probing can then be sent back to Google/Apple/Microsoft as part of their Telemetry. The issue is that this probing is unique and can be used to uniquely identify a user and

track such user. Shops, for example, can use this technique to fingerprint customers including when they return, where they go in the shop and how long they stay at a particular place. There are several papers[^60]'[^61] and articles[^62] describing this issue in depth.

This allows them to provide accurate locations even when GPS is off, but it also allows them to keep a convenient record of all Wi-Fi Bluetooth devices all over the world. Which can then be accessed by them or third parties for tracking.

Note: If you have an Android smartphone, Google probably knows where it is no matter what you do. You cannot really trust the settings. The whole operating system is built by a company that wants your data. Remember that if it is free then you are the product.

But that is not what all those Wi-Fi access points can do. Recently developed techs could even allow someone to track your movements accurately just based on radio interferences. What this means is that it is possible to track your movement inside a room/building based on the radio signals passing through. This might seem like a tinfoil hat conspiracy theory claim but here are the references[^63] with demonstrations showing this tech in action: http://rfpose.csail.mit.edu/ [[Archive.org]][58] and the video here: https://www.youtube.com/watch?v=HgDdaMy8KNE [[Invidious]][59]

Other researchers have found a way to count the people in a defined space using only Wi-Fi, see https://www.news.ucsb.edu/2021/020392/dont-fidget-wifi-will-count-you [[Archive.org]][60]

You could therefore imagine many use cases for such technologies like recording who enters specific buildings/offices (hotels, hospitals, or embassies for instance) and then discover who meets who and thereby tracking them from outside. Even if they have no smartphone on them.

![][61]

Again, such an issue could only be mitigated by being in a room/building that would act as a Faraday cage.

Here is another video of the same kind of tech in action: https://www.youtube.com/watch?v=FDZ39h-kCS8 [[Invidious]][62]

See [Appendix N: Warning about smartphones and smart devices]

There is not much you can do about these. Besides being non-identifiable in the first place.

Malicious/Rogue Wi-Fi Access Points:

These have been used at least since 2008 using an attack called "Jasager"[^64] and can be done by anyone using self-built tools or using commercially available devices such as Wi-Fi Pineapple[^65].

Here are some videos explaining more about the topic:

- HOPE 2020, https://archive.org/details/hopeconf2020/20200725_1800_Advanced_Wi-Fi_Hacking_With_%245_Microcontrollers.mp4
- YouTube, Hak5, Wi-Fi Pineapple Mark VII https://www.youtube.com/watch?v=7v3JR4Wlw4Q [[Invidious]][63]

These devices can fit in a small bag and can take over the Wi-Fi environment of any place within their range. For instance, a Bar/Restaurant/Café/Hotel Lobby. These devices can force Wi-Fi clients to disconnect from their current Wi-Fi (using de-authentication, disassociation attacks[^66]) while spoofing the normal Wi-Fi networks at the same location. They will continue to perform this attack until your computer, or you decide to try to connect to the rogue AP.

These devices can then mimic a captive portal[^67] with the exact same layout as the Wi-Fi you are trying to access (for instance an Airport Wi-Fi registration portal). Or they could just give you unrestricted access internet that they will themselves get from the same place.

Once you are connected through the Rogue AP, this AP will be able to execute various man-in-the-middle attacks to perform analysis on your traffic. These could be malicious redirections or simple traffic sniffing. These can then easily identify any client that would for instance try to connect to a VPN server or the Tor Network.

This can be useful when you know someone you want to de-anonymize is in a crowded place, but you do not know who. This would allow such an adversary to possibly fingerprint any website you visit despite the use of HTTPS, DoT, DoH, ODoH, VPN, or Tor using traffic analysis as pointed above in the DNS section.

These can also be used to carefully craft and serve you advanced phishing webpages that would harvest your credentials or try to make you install a malicious certificate allowing them to see your encrypted traffic.

How to mitigate those? If you do connect to a public wi-fi access point, use Tor, or use a VPN and then Tor (Tor over VPN) or even (VPN over Tor) to obfuscate your traffic from the rogue AP while still using it.

Your Anonymized Tor/VPN traffic:

Tor and VPNs are not silver bullets. Many advanced techniques have been developed and studied to de-anonymize encrypted Tor traffic over the years[^68]. Most of those techniques are Correlation attacks that will correlate your network traffic in one way or another to logs or datasets. Here are some examples:

- **Correlation Fingerprinting Attack:** As illustrated (simplified) below, this attack will fingerprint your encrypted Tor traffic (like the websites you visited) based on the analysis

of your encrypted traffic without decrypting it. Some of those methods can do so with a 96% success rate **in a closed-world setting**. **The efficacy of those methods in a real open-world setting has not been demonstrated yet and would probably require tremendous resources computing power making it very unlikely that such techniques would be used by a local adversary in the near future.** Such techniques could however hypothetically be used by an advanced and probably global adversary with access to your source network to determine some of your activity. Examples of those attacks are described in several research papers[^69]'[^70]'[^71] as well as their limitations[^72]. The Tor Project itself published an article about these attacks with some mitigations: https://blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations [[Archive.org]][64].



- **Correlation Timing Attacks:** As illustrated (simplified) below, an adversary that has access to network connection logs (IP or DNS for instance, remember that most VPN servers and most Tor nodes are known and publicly listed) at the source and the destination could correlate the timings to de-anonymize you without requiring any access to the Tor or VPN network in between. A real use case of this technique was done by the FBI in 2013 to de-anonymize[^73] a bomb threat hoax at Harvard University.



- **Correlation Counting Attacks:** As illustrated (simplified) below, an adversary that has no access to detailed connection logs (cannot see that you used Tor or Netflix) but has access to data counting logs could see that you have downloaded 600MB on a specific time/date that matches the 600MB upload at the destination. This correlation can then be used to de-anonymize you over time.



There are ways to mitigate these such as:

- Do not use Tor/VPNs to access services that are on the same network (ISP) as the destination service. For example, do not connect to Tor from your University Network to access a University Service anonymously. Instead, use a different source point (such as a public Wi-Fi) that cannot be correlated easily by an adversary.
- Do not use Tor/VPN from an obviously heavily monitored network (such as a corporate/governmental network) but instead try to find an unmonitored network such as a public Wi-Fi or a residential Wi-Fi.
- Consider the use of multiple layers (such as what will be recommended in this guide later: VPN over Tor) so that an adversary might be able to see that someone connected to the service through Tor but will not be able to see that it was you because you were connected to a VPN and not the Tor Network.

Be aware again that this might not be enough against a motivated global adversary[^74] with wide access to global mass surveillance. Such an adversary might have access to logs no matter where you are and could use those to de-anonymize you. **These adversaries are out of the scope of this guide.**

Be also aware that all the other methods described in this guide such as Behavioral analysis can also be used to deanonymize Tor users indirectly (see further [Your Digital Fingerprint, Footprint, and Online Behavior][Your Digital Fingerprint, Footprint, and Online Behavior:]).

I also strongly recommend reading this very good, complete, and thorough (and more detailed) guide on most known Attack Vectors on Tor: https://github.com/Attacks-on-Tor/Attacks-on-Tor [[Archive.org]][68] as well as this recent research publication https://www.researchgate.net/publication/323627387_Shedding_Light_on_the_Dark_Corners_of_the_Internet_A_Survey_of_Tor_Research [[Archive.org]][69]

As well as this great series of blog posts: https://www.hackerfactor.com/blog/index.php?/archives/906-Tor-0day-The-Management-Vulnerability.html [[Archive.org]][70]

Lastly, do remember that using Tor can already be considered suspicious activity[^75], and its use could be considered malicious by some[^76].

This guide will later propose some mitigations to such attacks by changing your origin from the start (using public wi-fi's for instance). Remember that such attacks are usually carried by highly skilled, highly resourceful, and motivated adversaries and are out of scope from this guide.

Disclaimer: it should also be noted that Tor is not designed to protect against a global adversary. For more information see https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf [[Archive.org]][71] and specifically, "Part 3. Design goals and assumptions.".

Some Devices can be tracked even when offline:

You have seen this in action/spy/Sci-Fi movies and shows, the protagonists always remove the battery of their phones to make sure it cannot be used. Most people would think that's overkill. Well, unfortunately, no, this is now becoming true at least for some devices:

- iPhones and iPads (IOS 13 and above)[^77]'[^78]
- Samsung Phones (Android 10 and above)[^79]
- MacBooks (macOS 10.15 and above)[^80]

Such devices will continue to broadcast identity information to nearby devices even when offline using Bluetooth Low-Energy[^81]. They do not have access to the devices directly (which are not connected to the internet) but instead use BLE to find them through other nearby devices[^82]. They are using peer-to-peer short-range Bluetooth communication to broadcast their status through nearby online devices.

They could now find such devices and keep the location in some database that could then be used by third parties or themselves for various purposes (including analytics, advertising, or evidence/intelligence gathering).

See [Appendix N: Warning about smartphones and smart devices]

TLDR: Do not take such devices with you when conducting sensitive activities.

Your Hardware Identifiers:

Your IMEI and IMSI (and by extension, your phone number):

The IMEI (International Mobile Equipment Identity[^83]) and the IMSI (International Mobile Subscriber Identity[^84]) are unique numbers created by cell phone manufacturers and cell phone operators.

The IMEI is tied directly to the phone you are using. This number is known and tracked by the cell phone operators and known by the manufacturers. Every time your phone connects to the mobile network, it will register the IMEI on the network along with the IMSI (if a SIM card is inserted but that is not even needed). It is also used by many applications (Banking apps abusing the phone permission on Android for instance[^85]) and smartphone Operating Systems (Android/IOS) for identification of the device[^86]. It is possible but difficult (and not illegal in many jurisdictions[^87]) to change the IMEI on a phone but it is probably easier and cheaper to just find and buy some old (working) Burner phone for a few Euros (this guide is for Germany remember) at a flea market or some random small shop.

The IMSI is tied directly to the mobile subscription or pre-paid plan you are using and is tied to your phone number by your mobile provider. The IMSI is hardcoded directly on the SIM card and cannot be changed. Remember that every time your phone connects to the mobile network, it will also register the IMSI on the network along with the IMEI. Like the IMEI, the IMSI is also being used by some applications and smartphone Operating systems for identification and is being tracked. Some countries in the EU for instance maintain a database of IMEI/IMSI associations for easy querying by Law Enforcement.

Today, giving away your (real) phone number is the same or better than giving away your Social Security number/Passport ID/National ID.

The IMEI and IMSI can be traced back to you in at least six ways:

- The mobile operator subscriber logs will usually store the IMEI along with the IMSI and their subscriber information database. If you use a prepaid anonymous SIM (anonymous IMSI but with a known IMEI), they could see this cell belongs to you if you used that cell phone before with a different SIM card (different anonymous IMSI but same known IMEI).
- The mobile operator antenna logs will conveniently keep a log of which IMEI and IMSI also keep some connection data. They know and log for instance that a phone with this IMEI/IMSI combination connected to a set of Mobile antennas and how powerful the signal to each of those antennas were allowing easy triangulation/geolocation of the signal. They also know which other phones (your real one for instance) connected at the same time to the same antennas with the same signal which would make it possible to know precisely that this "burner phone" was always connected at the same place/time than this other "known phone" which shows up every time the burner phone is being used. This information can be used by various third parties to geolocate/track you quite precisely[^88]'[^89].
- The manufacturer of the Phone can trace back the sale of the phone using the IMEI if that phone was bought in a non-anonymous way. Indeed, they will have logs of each phone sale (including serial number and IMEI), to which shop/person to whom it was sold. And if you are using a phone that you bought online (or from someone that knows you). It can be traced to you using that information. Even if they do not find you on CCTV[^90] and you bought the phone using cash, they can still find what other phone (your real one in your pocket) was there (in that shop) at that time/date by using the antenna logs.
- The IMSI alone can be used to find you as well because most countries now require customers to provide an ID when buying a SIM card (subscription or pre-paid). The IMSI is then tied to the identity of the buyer of the card. In the countries where the SIM can still be bought with cash (like the UK), they still know where (which shop) it was bought and when. This information can then be used to retrieve information from the shop itself (such as CCTV footage as for the IMEI case). Or again the antenna logs can also be used to figure out which other phone was there at the moment of the sale.
- The smartphone OS makers (Google/Apple for Android/IOs) also keep logs of IMEI/IMSI identifications tied to Google/Apple accounts and which user has been using them. They too can trace back the history of the phone and to which accounts it was tied in the past[^91].
- Government agencies around the world interested in your phone number can and do use[^92] special devices called "IMSI catchers"[^93] like the Stingray[^94] or more recently the Nyxcell[^95]. These devices can impersonate (to spoof) a cell phone Antenna and force a specific IMSI (your phone) to connect to it to access the cell network. Once they do, they will be able to use various MITM[^96] (Man-In-The-Middle Attacks) that will allow them to:
  - Tap your phone (voice calls and SMS).
  - Sniff and examine your data traffic.
  - Impersonate your phone number without controlling your phone.

- ...

Here is also a good YouTube video on this topic: DEFCON Safe Mode - Cooper Quintin - Detecting Fake 4G Base Stations in Real-Time https://www.youtube.com/watch?v=siCk4pGGcqA [[Invidious]][72]

For these reasons, it is crucial to get dedicated an anonymous phone number and/or an anonymous burner phone with an anonymous pre-paid sim card that is not tied to you in any way (past or present) for conducting sensitive activities (See more practical guidance in [Getting an anonymous Phone number][Getting an anonymous Phone number:] section).

While there are some smartphones manufacturers like Purism with their Librem series[^97] who claim to have your privacy in mind, they still do not allow IMEI randomization which I believe is a key anti-tracking feature that should be provided by such manufacturers. While this measure will not prevent IMSI tracking within the SIM card, it would at least allow you to keep the same "burner phone" and only switch SIM cards instead of having to switch both for privacy.

See [Appendix N: Warning about smartphones and smart devices]

Your Wi-Fi or Ethernet MAC address:

The MAC address[^98] is a unique identifier tied to your physical Network Interface (Wired Ethernet or Wi-Fi) and could of course be used to track you if it is not randomized. As it was the case with the IMEI, manufacturers of computers and network cards usually keep logs of their sales (usually including things like serial number, IMEI, Mac Addresses, ...) and it is possible again for them to track where and when the computer with the MAC address in question was sold and to whom. Even if you bought it with cash in a supermarket, the supermarket might still have CCTV (or a CCTV just outside that shop) and again the time/date of sale could be used to find out who was there using the Mobile Provider antenna logs at that time (IMEI/IMSI).

Operating Systems makers (Google/Microsoft/Apple) will also keep logs of devices and their MAC addresses in their logs for device identification (Find my device type services for example). Apple can tell that the MacBook with this specific MAC address was tied to a specific Apple Account before. Maybe yours before you decided to use the MacBook for sensitive activities. Maybe to a different user who sold it to you but remembers your e-mail/number from when the sale happened.

Your home router/Wi-Fi access point keeps logs of devices that are registered on the Wi-Fi, and these can be accessed too to find out who has been using your Wi-Fi. Sometimes this can be done remotely (and silently) by the ISP depending on if that router/Wi-Fi access point is being "managed" remotely by the ISP (which is often the case when they provide the router to their customers).

Some commercial devices will keep a record of MAC addresses roaming around for various purposes such as road congestion[^99].

So, it is important again not to bring your phone along when/where you conduct sensitive activities. If you use your own laptop, then it is crucial to hide that MAC address (and Bluetooth address) anywhere you use it and be extra careful not to leak any information. Thankfully many recent OSes now feature or allow the possibility to randomize MAC addresses (Android, IOS, Linux, and Windows 10) with the notable exception of macOS which does not support this feature even in its latest Big Sur version.

See [Appendix N: Warning about smartphones and smart devices]

Your Bluetooth MAC address:

Your Bluetooth MAC is like the earlier MAC address except it is for Bluetooth. Again, it can be used to track you as manufacturers and operating system makers keep logs of such information. It could be tied to a sale place/time/date or accounts and then could be used to track you with such information, the shop billing information, the CCTV, or the mobile antenna logs in correlation.

Operating systems have protections in place to randomize those addresses but are still subject to vulnerabilities[^100].

For this reason, and unless you really need those, you should just disable Bluetooth completely in the BIOS/UEFI settings if possible or in the Operating System otherwise.

On Windows 10, you will need to disable and enable the Bluetooth device in the device manager itself to force randomization of the address for next use and prevent tracking.

In general, this should not be too much of a concern compared to MAC Addresses. BT Addresses are randomized quite often.

See [Appendix N: Warning about smartphones and smart devices]

Your CPU:

All modern CPUs[^101] are now integrating hidden management platforms such as the now infamous Intel Management Engine[^102] and the AMD Platform Security Processor[^103].

Those management platforms are small operating systems running directly on your CPU as long as they have power. These systems have full access to your computer's network and could be accessed by an adversary to de-anonymize you in various ways (using direct access or using malware for instance) as shown in this enlightening video: BlackHat, How to Hack a Turned-Off Computer, or Running Unsigned Code in Intel Management Engine

https://www.youtube.com/watch?v=mYsTBPqbya8 [[Invidious]][73].

These have already been affected by several security vulnerabilities in the past[^104] that allowed malware to gain control of target systems. These are also accused by many privacy actors including the EFF and Libreboot of being a backdoor into any system[^105].

There are some not so straightforward ways[^106] to disable the Intel IME on some CPUs and you should do so if you can. For some AMD laptops, you can disable it within the BIOS settings by disabling PSP.

Note that to AMD's defense, so far and AFAIK, there were no security vulnerabilities found for ASP and no backdoors either: See https://www.youtube.com/watch?v=bKH5nGLgi08&t=2834s [[Invidious]][74]. In addition, AMD PSP does not provide any remote management capabilities contrary to Intel IME.

If you are feeling a bit more adventurous, you could install your own BIOS using Libreboot[^107] or Coreboot[^301] if your laptop supports it (be aware that Coreboot does contain some propriety code unlike its fork Libreboot).

In addition, some CPUs have unfixable flaws (especially Intel CPUs) that could be exploited by various malware. Here is a good current list of such vulnerabilities affecting recent widespread CPUs: https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability [[Wikiless]][75] [[Archive.org]][76]

Check yourself:

- If you are using Linux you can check the vulnerability status of your CPU to Spectre/Meltdown attacks by using https://github.com/speed47/spectre-meltdown-checker [[Archive.org]][77] which is available as a package for most Linux distros including Whonix.
- If you are using Windows, you can check the vulnerability status of your CPU using inSpectre https://www.grc.com/inspectre.htm [[Archive.org]][78]

Some of these can be avoided using Virtualization Software settings that can mitigate such exploits. See this guide for more information https://www.whonix.org/wiki/Spectre_Meltdown [[Archive.org]][79] (warning: these can severely impact the performance of your VMs).

I will therefore mitigate some of these issues in this guide by recommending the use of virtual machines on a dedicated anonymous laptop for your sensitive activities that will only be used from an anonymous public network.

In addition, I will recommend the use of AMD CPUs vs Intel CPUs.

Your Operating Systems and Apps telemetry services:

Whether it is Android, iOS, Windows, macOS, or even Ubuntu. Most popular Operating Systems now collect telemetry information by default even if you never opt-in or opted-out[^111] from the start. Some like Windows will not even allow disabling telemetry completely without some technical tweaks. This information collection can be extensive and include a staggering number of details (metadata and data) on your devices and their usage.

Here are good overviews of what is being collected by those five popular OSes in their last versions:

- Android/Google:
  - Just have a read at their privacy policy https://policies.google.com/privacy [[Archive.org]][80]
  - School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google https://www.scss.tcd.ie/doug.leith/apple_google.pdf [[Archive.org]][81]
- IOS/Apple:
  - More information at https://www.apple.com/legal/privacy/en-ww/ [[Archive.org]][82] and https://support.apple.com/en-us/HT202100 [[Archive.org]][83]
  - School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google https://www.scss.tcd.ie/doug.leith/apple_google.pdf [[Archive.org]][81]
  - Apple does claim[^108] that they anonymize this data using differential privacy[^109] but you will have to trust them on that.
- Windows/Microsoft:
  - Full list of required diagnostic data: https://docs.microsoft.com/en-us/windows/privacy/required-windows-diagnostic-data-events-and-fields-2004 [[Archive.org]][84]
  - Full list of optional diagnostic data: https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data [[Archive.org]][85]
- macOS:
  - More details on https://support.apple.com/guide/mac-help/share-analytics-information-mac-apple-mh27990/mac [[Archive.org]][86]
- Ubuntu:
  - Ubuntu despite being a Linux distribution also collects Telemetry Data nowadays. This data however is quite limited compared to the others. More details on https://ubuntu.com/desktop/statistics [[Archive.org]][87]

Not only are Operating Systems gathering telemetry services but so are Apps themselves like Browsers, Mail Clients, and Social Networking Apps installed on your system.

It is important to understand that this telemetry data can be tied to your device and help de-anonymizing you and later can be used against you by an adversary that would get access to this data.

This does not mean for example that Apple devices are terrible choices for good Privacy (tho this might be changing[^110]), but they are certainly not the best choices for (relative) Anonymity. They might protect you from third parties knowing what you are doing but not from themselves. In all likelihood, they certainly know who you are.

Later in this guide, we will use all the means at our disposal to disable and block as much telemetry as possible to mitigate this attack vector in the Operating Systems supported in this guide. These will include Windows, macOS, and even Linux in some regard.

See [Appendix N: Warning about smartphones and smart devices]

Your Smart devices in general:

You got it; your smartphone is an advanced spying/tracking device that:

- Records everything you say at any time ("Hey Siri", "Hey Google").
- Records your location everywhere you go.
- Always records other devices around you (Bluetooth devices, Wi-Fi Access points).
- Records your habits and health data (steps, screen time, exposure to diseases, connected devices data)
- Records all your network locations.
- Records all your pictures and videos (and most likely where they were taken).
- Has most likely access to most of your known accounts including social media, messaging, and financial accounts.

Data is being transmitted even if you opt-out[^111], processed, and stored indefinitely (most likely unencrypted[^112]) by various third parties[^113].

But that is not all, this section is not called "Smartphones" but "Smart devices" because it is not only your smartphone spying on you. It is also every other smart device you could have:

- Your Smart Watch? (Apple Watch, Android Smartwatch ...)
- Your Fitness Devices and Apps[^114]'[^115]? (Strava[^116]'[^117], Fitbit[^118], Garmin, Polar[^119], ...)
- Your Smart Speaker? (Amazon Alexa[^120], Google Echo, Apple Homepod ...)
- Your Smart Transportation? (Car? Scooter?)
- Your Smart Tags? (Apple AirTag, Galaxy SmartTag, Tile...)

- Your Car? (Yes, most modern cars have advanced logging/tracking features these days[^121])
- Any other Smart device? There are even convenient search engines dedicated to finding them online:
  - https://www.shodan.io/
  - https://censys.io/
  - https://www.zoomeye.org/

See [Appendix N: Warning about smartphones and smart devices]

Conclusion: Do not bring your smart devices with you when conducting sensitive activities.

Yourself:

Your Metadata including your Geo-Location:

Your metadata is all the information about your activities without the actual content of those activities. For instance, it is like knowing you had a call from an oncologist before then calling your family and friends successively. You do not know what was said during the conversation, but you can guess what it was just from the metadata[^122].

This metadata will also often include your location that is being harvested by Smartphones, Operating Systems (Android[^123]/IOS), Browsers, Apps, Websites. Odds are several companies are knowing exactly where you are at any time[^124] because of your smartphone[^125].

This location data has been used in many judicial cases[^126] already as part of "geofencing warrants" [^127] that allow law enforcement to ask companies (such as Google/Apple) a list of all devices present at a certain location at a certain time. In addition, this location data is even sold by private companies to the military who can then use it conveniently[^128]. These warrants are becoming widely used by law enforcement[^129]'[^130]'[^131].

If you want to experience yourself what a "geofencing warrant" would look like, here is an example: https://wigle.net/.

Now let us say you are using a VPN to hide your IP. The social media platform knows you were active on that account on November 4th from 8 am to 1 pm with that VPN IP. The VPN allegedly keeps no logs and cannot trace back that VPN IP to your IP. Your ISP however knows (or at least can know) you were connected to that same VPN provider on November 4th from 7:30 am to 2 pm but does not know what you were doing with it.

The question is: Is there someone somewhere that would have both pieces of information available[^132] for correlation in a convenient database?

Have you heard of Edward Snowden[^133]? Now is the time to google him and read his book[^134]. Also read about XKEYSCORE[^135]'[^136], MUSCULAR[^137], SORM[^138], Tempora[^139] , and PRISM[^140].

See "We kill people based on Metadata"[^141] or this famous tweet from the IDF https://twitter.com/idf/status/1125066395010699264 [[Archive.org]][88] [[Nitter]][89].

See [Appendix N: Warning about smartphones and smart devices]

Your Digital Fingerprint, Footprint, and Online Behavior:

This is the part where you should watch the documentary "The Social Dilemma"[^142] on Netflix as they cover this topic much better than anyone else IMHO.

This includes is the way you write (stylometry) [^143]'[^144], the way you behave[^145]'[^146]. The way you click. The way you browse. The fonts you use on your browser[^147]. Fingerprinting is being used to guess who someone is by the way that user is behaving. You might be using specific pedantic words or making specific spelling mistakes that could give you away using a simple Google search for similar features because you typed comparably on some Reddit post 5 years ago using a not so anonymous Reddit account[^148]. The words you type in a search engine alone can be used against you as the authorities now have warrants to find users who used specific keywords in search engines[^149].

Social Media platforms such as Facebook/Google can go a step further and can register your behavior in the browser itself. For instance, they can register everything you type even if you do not send it / save it. Think of when you draft an e-mail in Gmail. It is saved automatically as you type. They can register your clicks and cursor movements as well.

All they need to achieve this in most cases is Javascript enabled in your browser (which is the case in most Browsers including Tor Browser by default). Even with Javascript disabled, there are still ways to fingerprint you[^150].

While these methods are usually used for marketing purposes and advertising, they can also be a useful tool for fingerprinting users. This is because your behavior is unique or unique enough that over time, you could be de-anonymized.

Here are some examples:

- Specialized companies are selling to, for example, law enforcement agencies products for analyzing social network activities such as https://mediasonar.com/ [[Archive.org]][90]
- For example, as a basis of authentication, a user's typing speed, keystroke depressions, patterns of error (say accidentally hitting an "l" instead of a "k" on three out of every seven transactions) and mouse movements establish that person's unique pattern of behavior[^151]. Some commercial services such as TypingDNA (https://www.typingdna.com/ [[Archive.org]][91]) even offer such analysis as a replacement for two-factor authentications.
- This technology is also widely used in CAPTCHAS[^369] services to verify that you are "human" and can be used to fingerprint a user.
- See [Appendix A4: Counteracting Forensic Linguistics].

Analysis algorithms could then be used to match these patterns with other users and match you to a different known user. It is unclear whether such data is already used or not by Governments and Law Enforcement agencies, but it might be in the future. And while this is mostly used for advertising/marketing/captchas purposes now. It could and probably will be used for investigations in the short or mid-term future to deanonymize users.

Here is a fun example you try yourself to see some of those things in action: https://clickclickclick.click (no archive links for this one sorry). You will see it becoming interesting over time (this requires Javascript enabled).

Here is also a recent example just showing what Google Chrome collects on you: https://web.archive.org/web/https://pbs.twimg.com/media/EwiUNH0UYAgLY7V?format=jpg&name=4096x4096

Here are some other resources on the topic if you cannot see this documentary:

- 2017, Behavior Analysis in Social Networks, https://link.springer.com/10.1007/978-1-4614-7163-9_110198-1 [[Archive.org]][92]
- 2017, Social Networks and Positive and Negative Affect https://www.sciencedirect.com/science/article/pii/S1877042811013747/pdf?md5=253d8f1bb615d5dee195d353dc077d46&pid=1-s2.0-S1877042811013747-main.pdf [[Archive.org]][93]
- 2015, Using Social Networks Data for Behavior and Sentiment Analysis https://www.researchgate.net/publication/300562034_Using_Social_Networks_Data_for_Behavior_and_Sentiment_Analysis [[Archive.org]][94]
- 2016, A Survey on User Behavior Analysis in Social Networks https://www.academia.edu/30936118/A_Survey_on_User_Behaviour_Analysis_in_Social_Networks [[Archive.org]][95]
- 2019, Influence and Behavior Analysis in Social Networks and Social Media https://sci-hub.se/10.1007/978-3-030-02592-2 [[Archive.org]][96]

Revision #1
Created 2021-11-18 23:17:05 UTC by tinfoil-hat
Updated 2021-11-19 00:23:49 UTC by tinfoil-hat