A comprehensive guide on privacy and mass surveillance in the modern era: understanding the dangers of your private data being public."

[2024-08-31 Sat 13:43]

Contents

1 Privacy

To be truly free, you should be ready to risk everything for freedom.

Pavel Durov

2 Why Privacy Matters

2.1 I have nothing to hide

2.2 Privacy is dead, there's no point

3 Methods of Tracking

This section will cover the most common methods of tracking on the internet. Learn how you can prevent them in [BROKEN LINK: Preventing].

4 Browser Privacy

Browsers are one of the biggest threats to internet privacy, luckily a few still respect it.

4.1 TOR

:ID: 12eb0bd5-981f-4d3e-b477-a4edb2da138e :BTYPE: manual :TITLE: TOR :CUSTOM$_{\text{ID}}$: privacy ,#+title: Tor ,#+date: ,#+filetags: :tor: ,#+identifier: 20241015T165623 ,#+STARTUP: n ,#+bibliography: references.bib

The Tor browser is known to be one of the most secure and private browsers in existence. The Tor browser is often used by those living in oppressive countries that attempt to hide or censor important information from their citizens.

When it comes to the "proper" way to use Tor, it can get quite confusing. Many different people have many different opinions on whats best, so it is important that everyone does their own research and base their opinions off of what they think is best.

Below are some opinions regarding the use of VPNS which is a highly debated topic.

,** Regarding VPN usage:

According to the official Tor guide and website, you can "very well decrease your anonymity" by using a VPN in addition to Tor. While in theory

a VPN should provide an extra layer of security, there are a few things that privacy-conscious users should keep in mind. One of the biggest mistakes a Tor user can make is choosing the wrong VPN provider. It is known that most VPN providers keep logs of both internet traffic and your payments, so it is extremely important that each user does their own research to determine which (if any) VPNs fit their threat model. If you would like a brief summary of the top privacy VPNs, you can read this section.

Another aspect Tor users need to remember when using a VPN is that a VPN acts as a permanent entry or as a permanent exit node. This means that your VPN endpoint can (in theory) become a single point of failure. At the end of the day, the use of a VPN can both greatly increase or greatly decrease a user's privacy; these risks should be heavily considered and researched before committing to any one way.

One big use case for VPNs with Tor is circumventing censorship. If an oppressive government blocks known Tor nodes (which is very common), a VPN can mask the true destination of a user's requests.

Whether or not to use a VPN depends on the user, their risk tolerance, and their adversary. As the Tor Foundation put it: ,#+BEGIN$_{\text{QUOTE}}$ "Who's your adversary? Against a global adversary with unlimited resources more hops make passive attacks (slightly) harder but active attacks easier as you are providing more attack surface and send out more data that can be used. Against colluding Tor nodes you are safer, against blackhat hackers who target Tor client code you are safer".(,) ,#+END$_{\text{QUOTE}}$

,** Bridges ** Please navigate to Link [2] for more information.

,** Timing attacks

A "Timing attack" is a method of deanonymization which works by observing the timing of data entering and leaving the network. Alone, these times are almost irrelevant however if an attacker controls both the entry and exit nodes (and the user is on unpatched / old software) an attacker can compare the times from these nodes and deanonymize the user. This type of attack has been seen in the wild and according to a Bleeping Computer article: "The documents related to the information provided strongly suggest that law enforcement agencies have repeated and successfully carried out timing analysis attacks against selected gate users for several years to deanonymize them," stated CCC's Matthias Marx." (, a)

While this attack has been used in the wild, the tor foundation has stated that they have done "extensive work to flag and remove bad relays has taken place in the past years" as well as "the version used by the deanonymized user was retired in June 2022 and has been replaced by the next-gen Ricochet-Refresh, which features Vanguards-lite protections against timing and guard

discovery attacks." (, a)

"Maybe, but timing attacks are something that happens when you are being targeted, specifically. There's a lot of misinformation about exit nodes. A snooping exit node cannot identify you. Tor uses perfect forward secrecy to prevent the exit node from seeing what the entry and intermediate nodes see. In other words, it makes it impossible for the exit node operator to find out where the data request originated from, especially if you're connecting to an HTTPS site because then they can't even see what you're doing. Using a VPN over Tor is going to prevent your circuit from changing. All of your nodes in the circuit are fixed. The only use this has is if, for some reason, a site is blocking all of Tor's exit nodes; you can use a VPN at the end. Other than this, it has no real purpose. If you're wanting more anonymity, use Tor over VPN. This prevents your real IP from ever connecting to the Tor network. It will also keep your ISP from seeing you use Tor. Also, using this method keeps the VPN separate from the Tor network. The VPN can't see your Tor activity, and Tor can't see the VPN, with the exception of the guard. This would make exploiting your VPN much harder because an adversary would have to compromise Tor first. The other method means your VPN is basically acting as a second exit node. All this to say, if you're just a general web browser, you can probably do whatever you want without being exploited. But if we assume someone is wanting to use a VPN to make themselves more anonymous to the outside world, then you would definitely want to connect to Tor through the VPN, not connect to the VPN through Tor. By the way, here's the link: Link". (, a)

,** SNDL ** SNDL (Save now, decrypt later), sometimes known as "Harvest now, decrypt later," was a concep first exposed by the Edward Snowden leaks in 2013 Link.

,** Misc See the Browser Comparison Tor

4.2 Browser Alternatives

,#+title: Browser Privacy ,#+date: ,#+filetags: :privacy: ,#+identifier: 20241018T174112 ,#+OPTIONS: date:nil toc:nil num:nil ,*** Arkenfox Arkenfox is my preferred hardened browser

,*** Librewolf

Librewolf is a more "user-friendly" version of arkenfox which doesnt require any modification of your firefox client or user.js, and tends to work out of the box.

,*** Brave Brave browser is a very popular choice for "privacy" since most people arent aware of a certain incident. The brave browser was caught

injecting their own affiliate crypto links into certain URLs without user consent. Here is the brave CEO's statemement on the issue: ,#+BEGIN$_{\text{QUOTE}}$ "The autocomplete default was inspired by search query clientid attribution | that all browsers do, but unlike keyword queries, a typed-in URL should go to the domain named, without any additions. Sorry for this mistake — we are clearly not perfect, but we correct course quickly. ,#+END$_{\text{QUOTE}}$

On top of this shady incident brave is still not a great browser, for example brave is a chromium based browser which means it is under the indirect control of Google. The monopoly of chromium needs to stop before we can see internet privacy become mainstream and achievable for anyone.

,*** Chrome If you care at all about privacy, you should never be using chrome, you should probably just uninstal the spyware if you have it.

,*** Mullvad

4.3 Ads and Tracking

:ID: c98e62f5-dccc-4872-b786-9e7d801927eb ,#+OPTIONS: date:nil toc:nil num:nil ,#+TITLE: Ads

Advertisements almost rely on tracking you in order to give you advertisements that match your hobbies / interests / whatever else you do on the internet.

When it comes to preventing tracking like this a vanilla Ublock works perfectly. Out of the box UBlock origin also works with youtube!

NOTE: If you do not click the link provided above **PLEASE** make sure you install **Ublock Origin** and not **Ublock**. The latter is not safe.

4.4 Do Not Track (DNT)

:ID: 2e90c671-db54-4d6f-b5fa-7c14e98b0113 ,#+TITLE: Do not track (DNT)

Almost every browser has the option to enable sending a "DNT" request when getting a webpage, while this seems like an obvious win... theres nothing actually enforcing a website to respect this request, in fact it just makes your fingerprint more unique since an average user has no idea this feature even exists.

A better option is to leave both of these options OFF, so you blend in with the rest of the internet.

`file:///home/j/Documents/notes/media/fig1`

This is an example screenshot from firefox, these options may be different or not exist on other browsers.

5 Browser Comparison

:ID: 7ffde81c-4a94-4516-aff6-1b3263d9589d ,#+OPTIONS: date:nil toc:nil num:nil ,#+TITLE: Browser Comparison - Privacy ,#+date: ,#+filetags: :privacy: ,#+identifier: 20241019T175950 ,#+STARTUP: align Here is an outline of different browsers and their privacy features.

,#+LATEX$_{\text{HEADER}}$: graphicx % Include this package for resizing ,#+ATTR$_{\text{LATEX}}$: :environment longtable :align |l|l|l|l|l|l|l|l| ,#+ATTR$_{\text{LATEX}}$: :width Resize to fit the text width

Browser	Tracking Protection	Search Engine	Fingerprint Protection
Chrome	Basic	Google	No
Firefox	Strong	DuckDuckGo	Yes
Safari	Moderate	DuckDuckGo	Some
Brave	Strong	Brave Search	Yes
Edge	Moderate	Bing	No
Tor Browser	Very Strong	DuckDuckgo	Yes
Vivaldi	Strong	DuckDuckGo	Yes
Opera	Moderate	DuckDuckGo	Some
DuckDuckGo Browser	Strong	DuckDuckGo	Yes

And search engines

,#+LATEX$_{\text{HEADER}}$: graphicx % Include this package for resizing ,#+ATTR$_{\text{LATEX}}$: :environment longtable :align |l|l|l|l|l|l|l|l| ,#+ATTR$_{\text{LATEX}}$: :width Resize the table to the text width

Search Engine	Data Collection	Tracking	Ads	Encryption	Privacy-Focused	Default Option
Google	Yes	Yes	Yes	Yes	No	No
Bing	Yes	Yes	Yes	Yes	No	No
DuckDuckGo	Minimal	No	No	Yes	Yes	Yes
Startpage	Minimal	No	No	Yes	Yes	No
Qwant	Minimal	No	Yes	Yes	Yes	No
Ecosia	Minimal	No	Yes	Yes	Yes	No
Yahoo	Yes	Yes	Yes	Yes	No	No
Swisscows	Minimal	No	No	Yes	Yes	No
Mojeek	Minimal	No	No	Yes	Yes	No

6 Operating Systems and Privacy

:ID: 2e454ce6-f081-4dc5-8a1f-e133c013aa3a ,#+TITLE: Operating systems

,** Windows [link h3ere]
,** Linux
[[2e454ce6-f081-4dc5-8a1f-e133c013aa3a][Linux]

7 DNS Privacy

:ID: dc29079d-2255-4ba0-b927-f5a149321045
,* DNS

In my experience, DNS (Domain Name Server) is often overlooked in conversations about privacy, especially when compared to something like a VPN or browser. However, DNS can make or break even the strongest privacy setup.

,** What is DNS?

DNS stands for "Domain Name System" which is one of the most important building blocks of the modern internet, but to understand what DNS is for we first need to know how computers communicate. Unlike humans, computers dont understand letters or words, so computers need a way to translate a domain name to an IP address, for example if I wanted to go to 'www.google.com' my computer would need to know the literal IP address of that server, this is where DNS comes into play. When you assign a DNS server to your computer you are essentially giving your computer a table of IPs mapped to domain names, for example the IP that corresponds to 'https://google.com'" is '142.250.190.132'. So a good DNS server would be able to point my request to "www.google.com" to its real IP '142.250.190.132' (Note: the formatting you see in IPV4 addressing is still heavily abstracted for human readability however that goes beyond the scope of this paper).

,** Privacy?

Now DNS is essential for any modern internet user, but how can it leak my information? Well first we need to cover the most popular DNS servers, these are 1.1.1.1 (Cloudflare) and 8.8.8.8 / 8.8.4.4 (Google).

Now that we've covered the most popular DNS servers lets talk about how a DNS query works. Say I set my DNS server to 1.1.1.1 and try to connect to 'www.google.com'. My computer will first query 1.1.1.1 and find the corresponding IP address for that domain name. Now here is where it is very important to remember, **A VPN DOES NOT HIDE THIS REQUEST**. Depending on the server you use, a DNS query might be logged and visible, this is why it is extremely important to use a secure DNS.

,*** DNS over TLS

As previously mentioned there are methods to encrypt DNS traffic to mitigate snooping, these are most commonly known as DoT, DoH or DNScrypt. According to a cloudflare blog post: "DNS over HTTPS / TLS solves this. These new protocols ensure that communication between your device and the resolver is encrypted, just like we've come to expect of HTTPS traffic".

,** Local DNS

If you have a fancy or modern router there is also a chance that you might automatically be assigned a local DNS. Depending on your subnetting this might look like '10.0.0.1' , '192.168.0.1' or even just a random local IP where the DNS server is hosted. If you are in a heavily censored country this can expose what sites you are attempting to visit even through a VPN or tor, however certain protocols can help encrypt these requests such as DoH, DoT or DNScrypt which encrypt DNS traffic.

,** Better DNS options

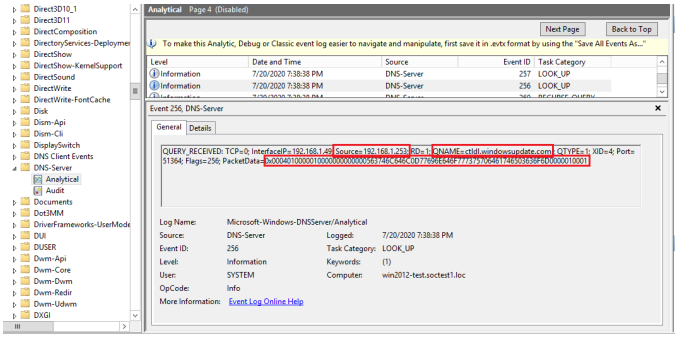
The most commonly used private DNS would be cloudflares 1.1.1.1. This is a good server to use if you dont want to worry about certain sites not loading as this server has a huge pool of IPs. Google DNS servers (8..8.8.8 and 8.8.4.4) claim to store no information so it shold be up to the users discretion to trust this claim, I personally prefer cloudflare or Quad9 though.

If you want maximum privacy Quad9 (9.9.9.9) can also be a good option but this is less mainstream so it might run into some lookup issues occasionally.

,** VPN DNS servers

The two best VPN providers (PIA and Mullvad) also come with their own private DNS servers. It would not be a bad idea to use these servers if you already use the VPN along with it, just remember to set your browser to the VPN DNS server (or set your browser to use the hosts DNS) or you will run into DNS issues when trying to connect to websites.

Sources (ignore) `https://blog.cloudflare.com/enable-private-dns-with-1-1-1-1-on-androi`
`https://cybersecthreat.com/2020/07/24/windows-dns-logging/` (



)

8 Preventing Tracking

8.1 Find My Info

8.2 VPNs

:ID: 7d63cb1c-8a60-4698-97e6-f691848051f8

,#+title: VPN ,#+date: *[2024-12-02 Mon 19:24]* ,#+filetags: :privacy: VPN ,#+identifier: 20241202T192427 ,#+EXPORT$_{\text{LATEX_CLASS}}$: article ,#+EXPORT$_{\text{OPTIONS}}$: toc:nil

PIA [BROKEN LINK: d260a8a9-bbed-4adf-a419-ddc444afd700] [BROKEN LINK: 9a5f0bff-4a2a-464c-8675-6a8317e2ceb4] [BROKEN LINK: 0b055dfe-4d02-4e73-a27b-570d5bfadf3f]

,* Introduction A Virtual Private Network (VPN) is a secure connection that allows you to browse the internet with enhanced privacy and security.

,* VPN Providers This section covers different VPN providers and their features.

,**Mullvad**

Mullvad is a privacy-focused VPN service that does not require an email address to sign up. It accepts anonymous payments and offers strong encryption. ,#+INCLUDE: "mullvad$_{\text{_privacy.org.gpg}}$"

For more information, visit the official Mullvad website:Mullvad VPN.

,**ExpressVPN**

is another popular VPN service that is known for its fast speeds and reliable performance.

More details can be found at the ExpressVPN website: ExpressVPN

8.3 Government Surveillance

8.3.1 NSA

This guide discusses various aspects of the Patriot Act

> "On April 24, 1996, President Bill Clinton signed the "Antiterrorism and Effective Death Penalty Act of 1996," to make it easier for law enforcement to identify and prosecute domestic and international terrorists. [1]

- allowing law enforcement to use surveillance and wiretapping to investigate terror-related crimes
- allowing federal agents to request court permission to use roving wiretaps to track a specific terrorist suspect
- allowing delayed notification search warrants to prevent a terrorist from learning they are a suspect
- allowing federal agents to seek federal court permission to obtain bank records and business records to aid in national - security terror investigations and prevent money laundering for terrorism financing
- improving information and intelligence sharing between government agencies
- providing tougher penalties for convicted terrorists and those who harbor them
- allowing search warrants to be obtained in any district where terror-related activity occurs, no matter where the warrant is executed
- ending the statute of limitations for certain terror-related crimes
- making it harder for aliens involved in terrorist activities to enter the United States
- providing aid to terrorism victims and public safety officers involved in investigating or preventing terrorism or responding to terrorist attacks [1]

> "According to a 2015 Washington Post article, the Justice Department admitted, "FBI agents can't point to any major terrorism cases they've cracked thanks to the key snooping powers in the Patriot Act." [1]

Another important aspect of the NSA survellence that Edward Snowden leaked is known as PRISM. PRISM was created in 2008 with the intention

of intercepting and storing "suspicious" communications. While it is clearly stated that they can only monitor "court approved" communications the [Edward Snowden Leaks] proved otherwise. According to an article published by The Guardian

> judges have signed off on broad orders which allow the NSA to make use of information "inadvertently" collected from domestic US communications without a warrant. 3

According to the official document:

> "The Government cannot target anyone under the court-approved procedures for Section 702 collection unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and the foreign target is reasonably believed to be outside the United States. We cannot target even foreign persons overseas without a valid foreign intelligence purpose." [3]

dni.gov 2013

1. Timeline **2001** September 11: Terrorist attacks on the World Trade Center and the Pentagon. September 13: Introduction of the Combating Terrorism Act by Senators Orrin Hatch and Jon Kyl. September 20: Introduction of the Public Safety and Cyber Security Enhancement Act by Rep. Lamar Smith. September 28: Introduction of the Intelligence to Prevent Terrorism Act by Senators Bob Graham and Jay Rockefeller. October: Proposal for the USA PATRIOT Act is drafted. October 26: USA PATRIOT Act signed into law.

   2004 April 9: ACLU files a lawsuit challenging parts of the USA PATRIOT Act. [1]

   2005 April: Senate Judicial Hearing on the USA PATRIOT Act. July 21: Select Committee on Intelligence proposes the USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005. Renewal of several provisions of the USA PATRIOT Act.

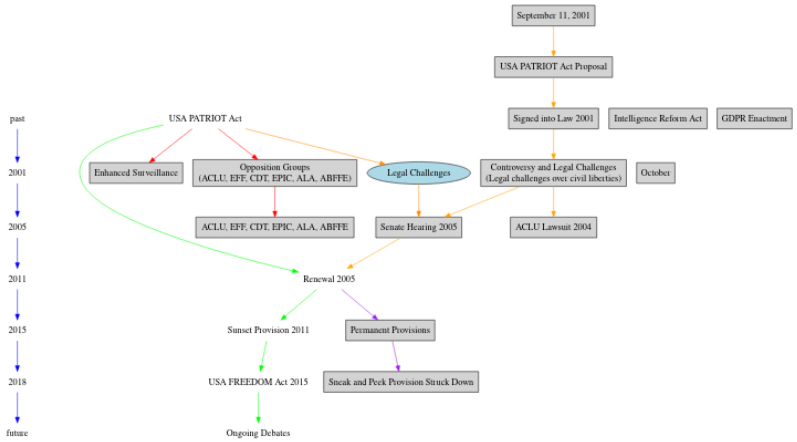
   2011

   - Sunset provisions of the USA PATRIOT Act come into effect, leading to debates on reauthorization.

2015 USA FREEDOM Act enacted, modifying some provisions of the USA PATRIOT Act.

2018 Further discussions on the implications of the USA PATRIOT Act and related laws. [3]

2. Timeline visual



8.3.2 GDPR

9 Citations

,#+title: Citations: ,#+OPTIONS: date:nil toc:nil num:nil

,**** [] History.com Editors, "Patriot Act," HISTORY, Aug. 21, 2018. `https://www.history.com/topics/21st-century/patriot-act`

,**** [] "The top secret rules that allow NSA to use US data without a warrant," the Guardian, Jun. 20, 2013. `https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant`

,**** [] "Reddit - Dive into anything," Reddit.com, 2024. `https://www.reddit.com/r/TOR/comments/1fsqk5p/comment/lpmg9x9/?utm_source=share&utm_medium=web3x&utm_name=web3xcss&utm_term=1&utm_content=share_button` (accessed Oct. 20, 2024).

,**** [] "BRIDGES." `http://dsbqrprgkqqifztta6h3w7i2htjhnq7d3qkh3c7gvc35e66rrcv66did.onion/bridges/index.html` (accessed Oct. 2024).

,**** [] B. Toulas, "Tor says it's 'still safe' amid reports of police deanonymizing users," BleepingComputer, Sep. 19, 2024. `https://www.bleepingcomputer.com/news/security/tor-says-its-still-safe-amid-reports-of-police-deanonymizing-users/` (accessed Oct. 20, 2024).

,**** [] “Facts on the Collection of Intelligence Pursuant to Section 702,” 2013. Available: https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

,**** [] Wikipedia Contributors, “History of the Patriot Act,” Wikipedia, Oct. 14, 2018. https://en.wikipedia.org/wiki/History_of_the_Patriot_Act

,**** [] “TorPlusVPN · Wiki · Legacy / Trac · GitLab,” GitLab, 2024. https://trac.torproject.org/projects/tor/wiki/doc/TorPlusVPN (accessed Oct. 20, 2024).

,* Unsorted citations ,**** https://www.pcmag.com/news/mullvad-vpn-hit-with-search-warra (Mullvad) ,**** https://arstechnica.com/information-technology/2021/09/privacy-focused-protonmail-provided-a-users-ip-address-to-authorities/ (mullvad)

,* Do ,* TODO use this https://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/ ,* TODO work on citations

,#+bibliography: references.bib