DECEMBER 2020

# PRIVACY 101

## AN INTRODUCTION ON HOW TO FIGHT AGAINST ONLINE INTRUSION

## WHY SHOULD I CARE?

# "I HAVE NOTHING TO HIDE"

Procrastination always helps finding the perfect excuse to avoid doing anything about whatever thing that is on our minds. But the phrase above is an old excuse that has been repeated in many different ways by extremely different people:

*"You have nothing to fear if you have nothing to hide" - Joseph Goebbels*

*"Anyone who is afraid now is guilty, for innocence never fears public surveillance" - Maximilian Robespierre*

*"The only people who don't want to disclose the truth are people with something to hide." - Barack Obama*[1]

Privacy is not an objective or an end, but the mean by which we think for ourselves, investigate and reach conclusions. Freedom of thought only occurs when we feel we are in a private environment. How many silly opinions did you first have about a subject before researching or thinking a bit more about it? Would you have been able to ask yourself all the embarrassing questions you had if everyone knew you were asking them? We censor ourselves and act differently when we think we are being supervised or while being part of a group.[2]

So... is there anything that we can do? What could possibly one individual do to defend themselves from the intrusion of the most powerful governments and companies in the world?

---

[1] In the context of the Citizens United Supreme Court case.

[2] Solomon Asch Conformity Experiment: https://www.simplypsychology.org/asch-conformity.html. Also carried out by YouTube Channel VSAUCE: https://youtu.be/fbyIYXEu-nQ

## THE POWER IS ON YOUR HANDS

# TAKE BACK CONTROL

What if there were gadgets, tools, programs and services that were custom made in order to help you take back your privacy? There is already a community of privacy minded people and companies trying to solve the surveillance problem through different hardware and software solutions. Here are some that will aid you in fighting back against government and corporate surveillance:

| | |
|---|---|
| Encryption | Private Cloud Services/File Encryption |
| VPN | Privacy Focused Hardware |
| Tor & Private Browsers | Pay To Use Business Model |
| Public DNS | Open Source Software |

Some of these solutions are free, some are cheap and some can be expensive. However, there are loads of different applications, services and products out there that vary in price and quality. You just need to look for them. While you still need to be careful and use tools that can be trusted, the fact that you are taking privacy into account when selecting a product, app or service, you are already making huge strides in a more private life. The recommendations made in this document regarding a specific product or provider are just that, recommendations. There is no silver bullet, no perfect piece of software. There are trade-offs with everything. The objective of this document is to inform you about concepts and options available, for you to then make your own decisions.

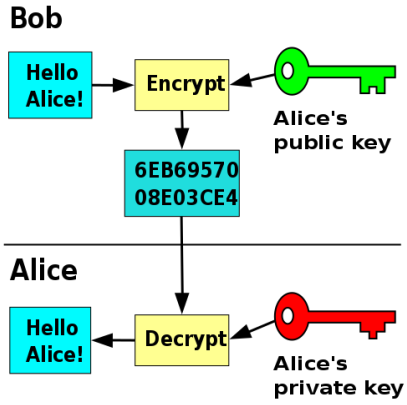
As a general rule, try not to have un-encrypted data stored in services based in the United Kingdom, United States, Australia, Canada, and New Zealand, since they share intelligence databases and can compel companies to surrender encryption keys.[3] But what is encryption?

---

https://www.privacytools.io/providers/#ukusa

# ENCRYPTION

Encryption predates the modern computer era. During WWII, the German army famously communicated using a device called Enigma. A machine that would encode messages in readable text or "plain-text" into unreadable text or "cypher-text". To read it, you would need a key that would decrypt the cypher text back to plain text. Even though technology has made encryption infinitely more advanced and complex, the concept remains pretty much the same:




Why isn't everything encrypted then? Well... encryption can be costly, in terms of resources and development: it slows down websites and it is not easy to implement.

Should a personal blog about kittens use encryption? What is the benefit of encrypting that content? Can the blogger pay for its cost? Will it slow down the website? What about your bank's website?

| Entity | Benefit of encryption? | Cost of encryption? | Slow down website? |
|---|---|---|---|
| Kitten Blog | Third parties will not know about the content you post, comment or like in the website. | Hiring a developer or service that can implement encryption on the blog | Since the website has lots of high quality images, with encryption they would take significantly longer to load. |
| Bank | Your financial data is secure. | Already hired development team implements encryption | Since the website has mostly texts and numbers, encryption does not increase load times significantly. |

The costs do not undermine the value of privacy though. This example is used to show that it is not as clear cut as "encrypt everything and problem solved".

On another note, encryption shifts the focus of security. There is no need for a 100% secure infrastructure (which is impossible to get anyways) when the information it holds is impossible to read anyways.

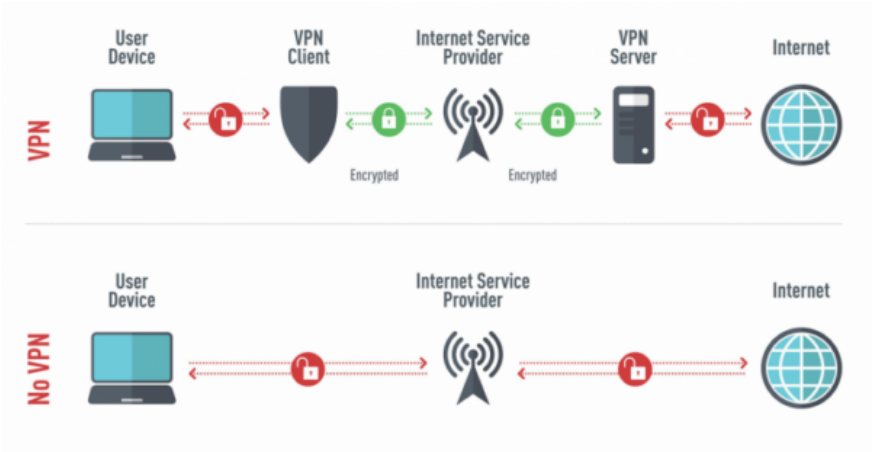
# VPN[4]

When we walk into a store or a supermarket, nobody knows the address to our home. But if you are browsing the Internet, every website can find where you are. This is due to your Internet Protocol address or IP address.

When you type in “www.google.com", your computer requests an IP address. Once you get that IP address, your computer sends a request with *your* IP address to that website, who sends its content back to your IP address.

A Virtual Private Network is a middle man that acts as your public face towards websites. Websites think your IP address is the one that belongs to your VPN server, so they send their content there. Privately, the VPN sends that content back to your IP address, without anyone else knowing what is your device’s online address.

If you ask a question to someone on the street, they see you, hear you, they can identify you. But if you ask a friend to ask someone a question, then your friend is the one who is recognizable and not you. Not clear enough? Take a look at this:




Your VPN faces your ISP and the Internet while keeping you hidden. VPN services also encrypt your requests, so they are not only private but also secure.

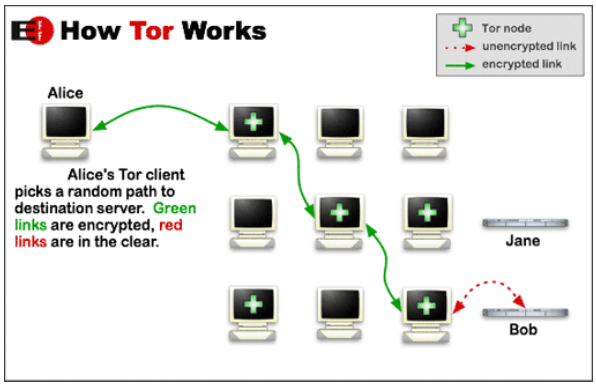
When looking for a VPN, make sure you choose one that has little to no history of security breaches and offers the features you need and like. ProtonVPN is a really good one, based in Switzerland. It also provides other services that will be mentioned in this document.

Are VPNs a silver bullet? Are they the only thing needed? Far from it, but they do play an enormous role in improving your privacy online.

[4] https://www.privacytools.io/providers/vpn/

# TOR & BROWSERS[5]

You probably heard of Tor in the news. It is the method that hackers, political activists and criminals use to navigate the Internet and share information. It sounds super scary! You do not want to be in the company of those kinds of people, you just want to talk to friends about sports and look at blooper videos. But all that Tor does is grant anonymity using a special network of relays:




You can still use Tor to access all the same sites you access regularly; if you do not want to buy or sell drugs just do not go to the drug dealer. As simple as in "real" life. This explanation does not do justice to what Tor is and how you would benefit from using it, so please investigate more! Check out what an Onion service is. If *it* hits the fan, Tor is your best chance at staying private and anonymous online. The easiest way to access the Tor network, is using the Tor browser.

Not convinced with Tor? There are some "mainstream", more well known options. Lookout for browsers that are centered around privacy. The biggest one is Mozilla Firefox, by the Mozilla Foundation. Unlike with Tor, you should install some add-ons and make some tweaks (which might be a little advanced for beginners). But add-ons are easy to install and use.[6]

If you are using Firefox or another privacy focused browser, remember to use a VPN! This is the difference with Tor: Tor is decentralized while the VPN relies on the VPN provider's servers. You do not need to trust Tor to use it, but you do need to trust the VPN provider since they hold the keys to the kingdom.

Oh and remember about DNS? You should also change that to a public one.

[5] https://www.privacytools.io/browsers/#browser

[6] https://www.privacytools.io/browsers/#addons

# PUBLIC DNS

Although DNS has already been mentioned in this document, here is a bit more information about it. Think of Domain Name System (DNS) as the phonebook (contact list for those who have never seen a phonebook) of the Internet. When you input an URL in your browser, how does it know where to go? Where to download the website from?

When you look for someone's number, you search for their name and get their phone number. For the Internet is the same, but instead of phone number you get an IP address. Your Internet Service Provider (ISP) provides this service using their own DNS which is often:

- Outdated: when it cannot find a website it bounces your request to other servers to find it.
- Unprotected: No phising protections, no encryption of your requests.
- Not private: your ISP can record the requests coming from your IP address to their DNS service.

So, how can you change it to a public DNS? This can be done on device level (i.e. computers, smartphones) or on a router level. Search for a quick guide using these keywords: "switch DNS [insert operating system]". You can do the same for your router, but it might be more difficult for the unexperienced.

Hang on, if it is public, then all your requests are public too! That is why you should you DNS over HTTPS (encrypted DNS).

# PRIVATE MESSAGING

The suggestion for private messaging is simple: the data has to be encrypted (duh!) and as much metadata **must** be encrypted as well. No Facebook product encrypts metadata and some questions are raised as to whether it even has end to end encryption. This include Facebook Messenger, WhatsApp and Instagram Messages. Facebook is not the only to not encrypt metadata and even store it, so what options are out there?

There is an app called Signal that is open source and has encryption all over it. It is available for almost any platform so give it a try and get your friends and family to start using it as well. FYI, Edward Snowden uses Signal.

But it does not have to be Signal. There are other options out there, with different advantages and disadvantages. Signal's main weakness is that is centralized, so perhaps you should check out some decentralized software options for real time chats.[7]

# PRIVATE CLOUD SERVICES/ENCRYPTING FILES

Did you know that Google can scan for the contest of any files you have stored in Google Drive? Sure, when you request to open a file, you do it through a secure connection (HTTPS) and you are authenticated. But the file is not encrypted in their servers, so with access to them, your files are free to be read, copied by anyone with access to Google's servers (like the NSA[8]).

So what is the solution? You can pay for a Cloud provider whose business model relies on receiving your monthly payments instead of accessing your data or/and you could encrypt your files yourself and upload them encrypted. There are many file encryption software options to choose[9], like 7-Zp for Linux and Windows or VeraCrypt, available for Linux, Windows and MacOS.

[7] https://www.privacytools.io/software/real-time-communication/

[8] https://en.wikipedia.org/wiki/Edward_Snowden#/media/File:NSA_Muscular_Google_Cloud.jpg

[9] https://www.privacytools.io/software/encryption-tools/

# PRIVACY FOCUSED HARDWARE

One of Edward Snowden's leaks showed that the NSA was using programs called Smurfs. Here are some Smurfs and what they can do:

Dreamy Smurf: turn on or off your phone without you knowing.

Nosey Smurf: turn on your mic and record everything it reaches it.

Tracker Smurf: a geolocation tool that is more precise than bouncing the telephone signal through cell towers (like the do in movies when they need to keep the bad guy on the phone for a few minutes).

Paranoid Smurf: helps the other Smurfs to stay undetected.

These programs could work on any type of device, smartphone or computer (they are the same for all intents and purposes). So what can you do? This one is tough, and there is no evidence that the NSA was using this tools on massive scale so we should be safe. Having said that, we can no longer trust our phones to be completely private, even if we are using a privacy minded, open source OS. Do not have your phone with you all the time.

For computers, there are some solutions. Most laptops come with webcam covers but some are also coming out with physical switches for the microphone, camera, WiFi and Bluetooth. With no electricity going through, those features cannot be turned on through any software program.

Most probably, you will not be subjected to a spyware attack with Smurfs or similar programs. So take at least the necessary precautions: use strong unique passwords (or even better, strong unique pass-phrases), encrypt your storage drives, among other practices. The internet is full of guides that you can follow[10], including this document. Educate yourself and use the tools at your disposal. It is possible to follow all of the privacy best practices without surrendering that much or any comfort at all. Besides, once you know how much your privacy is at risk you will appreciate any tool that helps you protect it.

[10] https://proprivacy.com/

# PAY TO USE BUSINESS MODEL

You should watch the documentary “The Social Dilemma”. In it, Jaron Lanier explains what is wrong with the business model that most of the big tech companies are using. Think about Google products, Facebook, among many others. How do they earn money? You do not pay to use them, they do not receive donations. So where is the money coming from?

Lanier does not think that this companies are necessarily evil, but they rely on the free to use business model. In order to provide a free service, these companies monetize your data while using their platforms. Data includes: the content users upload (pictures, comments, posts, audio, personal data like age or gender), metadata (activity records of everything you do on that platform) and the mixture of both: a virtual profile that they sell to advertisers. It is the business model that drives this companies to have these invasive software products.

The solution? Start using Pay to use services like Netflix and Spotify. Start switching to software created by foundations that rely on donations (those who donate cover the cost for those who do not). But most importantly, **delete** your social media accounts. There are other problems with social media that are not related to privacy as well, please watch “The Social Dilemma” for more information, it is a great way to kickstart you into this topic.

# OPEN SOURCE SOFTWARE

How on Earth is open source software better for privacy? Better for security?!

Contrary to intuition, actually having the source code at the disposal of the community, helps audit the code and remove security vulnerabilities and make it transparent. If the application is collecting your data, that command will show up in the source code. Nothing happens behind the scenes.

If you can, try to still pay for the software even if it is free. Make a donation. Nothing is free, someone (probably the developers working on the software’s code) is covering that cost for you.

## OK, WHAT NOW?

# THIS SHOULD ONLY BE THE BEGINNING

Anyone who reads this guide and is already “in” on privacy protection practices, will think this guide is oversimplifying lots of concepts and a bit naive in thinking that all this steps completely protect one’s privacy. And they would be right.

The purpose of this guide is to help people who know next to nothing about privacy and want to take steps to use the Internet better. Some people do not even know that they are not browsing privately.

To those people: welcome. Continue to ask questions, use critical thinking, continue to learn. Is any of the information in this guide correct? Is it up to date? Is that service provider safe? Are all operating systems safe and private? Having taken all this steps to browse safely with my computer, what about my phone? What are onion services in Tor? If onion services are not indexed by a search engine (e.g. Google Search), how do you use them? Shouldn’t network configurations be done on my router instead of doing it on each device?

Do not get frustrated, learning takes time and practice.

...

But whenever you do get frustrated and procrastination starts to kick in, imagine what would life be like if everyone knew all your Google searches. That they knew how long you stared at someone’s picture and which picture. If the local grocery shop knew what you did on your last Friday night or how much money you made last month. Do not hold different standards to your privacy online that the ones you hold for your “real” life.

Oh and by the way, did you know that the more people use the Tor network, the safer it gets?