

**Online security and anonymity**

**Matteo Gianvenuti**

Summary

[Introduction 3](#_Toc185939555)

[What identify and expose you online? 3](#_Toc185939556)

[Alternatives that protect you (from simple to complex) 4](#_Toc185939557)

[Virtual Private Network (VPN) 4](#_Toc185939558)

[Proxy server 4](#_Toc185939559)

[The Onion Router (Tor) 4](#_Toc185939560)

[Operative System (OS) 5](#_Toc185939561)

[Whonix 5](#_Toc185939562)

[Conclusion 5](#_Toc185939563)

[Bibliography 6](#_Toc185939564)

# Introduction

The private companies, the organizations and the government aim to collect as much information about you as possible—just like in all the precious years, of course. Now and in the future, this will be much easier. This is because everything is going digital, mainly through hardware devices and software applications that do not pursue the user’s interest. They are not designed to protect your data, block the tracking attempts, anonymize, or protect your identity; on the contrary, they do the opposite.

As immediate consequence, the problem of personal safety and so anonymity (especially online) nowadays is greater than ever, and it will continue to grow. Those who controls the information of an individual have the full control over them. In a world like this democracy no longer exists. There can be no opposition in a system where people are completely controlled.

For these reasons, in this course thesis, we will attempt to set up a secure workstation by analyzing the security of various privacy-focused technologies, such as VPNs, Tor, Whonix.

# What identify and expose you online?

* **IP address:** The IP address serves two main functions: network interface identification and location addressing. It allows the packets delivery from the source host to the destination host on the internet (also in a private network) then it uniquely identify you. This mean the online activity is linked to the IP address and from it to a person or at least to a device. The IP address is typically assigned by the internet provider (more properly the internet access provider or the Internet Service Provider also known as ISP).

According to Italian laws, the ISP have to collect lots of information on the users, like: Information about who communicated with whom (e.g., IP addresses, connection timestamps, and duration), the internet access logs (the data must be retained for 12 months, extendable in case of a “crime”) and much more.[[1]](#one)[[2]](#two)[[3]](#three)[[4]](#four)

* **Browser and browser fingerprint:** The browser configuration is important because through the browser set up is possible to understand who is. How many other users have your same configuration? This is the fingerprint; thanks to it you can easily distinguish between thousands of users when you are looking for someone. It contains also a lot of information about the device.

Even the browser itself is important, did you know that Google Chrome send to Google LLC all the URLs you visited? (until few years ago in EU) Instead, a privacy-focused browser does not collect any type of information on you, furthermore, with a good set up it can clean all your data after every session (the local data).

* **Cookies:** They are used to identify users and typically contain information about their identity, the site visited, and other related data. Cookies can track whether you have visited a specific site or even a particular page, including across different domains (e.g., third-party cookies). They monitor your behaviour.
* **Cross-site tracking and data aggregation:**
* **Application tracking:** Did you know that more than the 80% of the applications in the common stores like Google Play Store and Apple App Store contains a lot of trackers? They try to get as much as possible information on you, like: OS, CPU data, memory data, GPS position, IP address, network data, age, gender, address, and so on.[[5]](#five)
* **OS and device information:**
* **Social networks:** They are one of the most aggressive data collectors and even one of the most dangerous. Basing on how you interact with them, what you watch and in general what you do in the platform they can estimate a digital version of you; they may know you better than your friends if you gave them enough data. With these data they can manipulate and change the content you see and then change your mind.

Did you know that in the last Italian elections, a truly “anti-system” party was shadow banned? The elections were clearly influenced and manipulated, not only by social networks but also by Google and similar companies. That’s why I do not have any social network.

* **Metadata:** All the files contain some metadata. They are information like author, device, timestamp, geolocation, application used to create the file, etc. Then, remember this the next time you will upload a file online or on a social network. Do not the same mistake of John McAfee, Rocco Castoro, Robert King and Vice magazine.
* **Extra considerations:** In general, almost every entity that interacts with you collects data on you in an aggressive way. If I had to do a complete list of what identify you it may be infinite. Do consider, especially if you are not aligned with the establishment, all the data collected by almost all the big and small companies are completely available for the intelligence agencies.[[6]](#six)

# Alternatives that protect you (from simple to complex)

## Virtual Private Network (VPN)

## Proxy server

## The Onion Router (Tor)

## Operative System (OS)

## Whonix

# Conclusion

Pay attention at the services you use.

# Bibliography

[1] D.Lgs. 109/2008: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1607282>.

[2] D.Lgs. 196/2003: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196>.

[3] GDPR: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679>.

[4] Law 167/2017: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017;167>.

[5] You can check it with the anti-trackers integrated in the mobile browser DuckDuckGo or even better with TrackerControl form the F-Droid store.

[6] From “Errore di sistema” / “Permanent record” the Edward Snowden autobiography.

[7]