To put these guidelines into practice we suggest using software like these:

For messaging and phone calls: ***Signal*** ***and*** ***Matrix*** (decentralized)
To surf the internet: ***TOR***, ***Brave*** and ***Firefox***
Search engine (in place of Google Search for example): ***Duckduckgo***
Plug-in for your browser: ***Privacy Badger***, ***HTTPS Everywhere***, ***Facebook Container***
Encrypted email services: ***Protonmail*.com**, ***posteo.de***, ***tutanota.com***, ***mailbox.org***
Distributed social networks: ***Mastodon***, ***Diaspora***
Servizio di video decentralizzato: ***PeerTube*** (servers list)
Off-line maps, based on OpenStreetMap: ***OsmAnd***
Traduttore: ***Deepl.com***
Decentralized data processing and sharing service: ***Nextcloud***
Personal computer operating system: ***GNU/Linux***
Smartphones with Google-Free Android and GNU/Linux: ***/e/***, ***puri.sm***, ***tuxedocomputers***
Google-Free Android Operating system: ***LineageOS***
Password managers: ***KeePass, Firefox Password Manager***
Attend the shops in your ***community,*** rather than Amazon

Notes

(**1**) https://protonmail.com/blog/
(**2**) https://en.wikipedia.org/wiki/The_World%27s_Billionaires
(**3**) Permanent records. Edward Snowden, 2019. Metropolitan Books.
(**4**) Radical technologies. 2017, Verso Books.
(**5**) The age of surveillance capitalism. The Fight for a Human Future at the New Frontier of Power. Shoshana Zuboff. 2019, Ed. Public Affairs
(**6**) http://www.rai.it/programmi/ report/
(**7**) https://en.wikipedia.org/wiki/Free_and_open-source_software

Extended and updated version on miniguide.minifox.fr
Text edited by Francesco Reyes

Personal Data Protection Mini-Guide

for the protection of people and democracy (May/2020)

Spread of digital communications

The last 20 years have seen the spread of technologies based on internet connectivity, starting with smartphones and their applications: Whatsapp, Telegram, etc., e-mail services, search engines, maps, such as Google-Search, -Mail and -Map, with which to communicate or search for information apparently at "no cost".

In this period, companies such as Facebook (owner also of Whatsapp and Instagram), Google and Amazon have reached an exorbitant number of customers, greater than any nation state (up to 2.5 billion in the case of Facebook)[1].

"Zero cost"? The business of the Hi-Tech giants

In the years when global wealth has been concentrated in fewer and fewer hands, the owners of the Hi-Tech giants have become the richest men on the planet[2]. To give an example, in 2018 Google had a turnover of $136 billion, on average $91 for each of its Gmail users.

Although the products of these companies do not require direct payment in cash, they manage to extract huge amounts of capital from the population by selling information and behavioural profiles of their users to other companies. In addition, the massive transfer of data to governments[3] and illegal sales to private companies[1] has been documented several times.

Personal data (and metadata) released online

The data collected while using these computer tools may include what you write in messages or emails, what you say during a phone call, your sexual

preferences (e.g. Tinder), the internet pages you visit, your digital purchases, "likes" on Facebook, comments left on a blog.

In addition to this data, a great deal of technical information (called "metadata") is also collected, which reveals countless things about us and the context in which we communicated. The metadata is easy to analyze automatically (with computers) in order to know life habits, relationships and user preferences. The metadata collected includes the network of your contacts, the people you contact more and less, and those you don't talk to at all, the sequence of people who have shared the same message on WhatsApp, the movements of your finger or mouse on the screen when you visit a website equipped with tracking cookies (most sites use Google cookies[1]), the route described by your phone's GPS, the place where you connected to a Wifi network [4,5], ….

The data that we (involuntarily) gave away are no longer ours, but will belong to a "new owner" indefinitely, stored in some datacentre[3, 4].

How can the data business be profitable?

The data collected contains a detailed description of the society and the relationships between its members, the opinions and political positions of each citizen.

The possible uses of data like this are numerous. Given the cost and expertise needed to store and analyse this data, however, those who really exploit this mass data collection are generally large multinationals and secret services: the former for economic flow control purposes[5], the latter for political control and public opinion manipulation[3].

All of this happens almost invisibly because through technological systems with which we, average users, are not familiar. In addition, the verification of software by specialists is generally hindered by copyright or military secrets[4].

Among the possible uses of "mass data" in the company: beating the competition thanks to a detailed knowledge of our lives, convincing the user to buy certain products with advertising targeted at the individual, changing the price of a product based on our profile. In government: adapt political propaganda to the moods of the population in order to always appear to be winning, influence elections, foment or prevent riots, identify and suppress political opponents, steal scientific discoveries[6].

How to protect personal data and thus the democratic system

It is really not ok that a few very wealthy companies own and use information about every single person in the world to their advantage. This is especially true, given that the world's population cannot decide anything about the conduct of such companies. In a world where so much of our lives pass through digital tools, we should not let that information slip out of our hands, as we are the legitimate owners of our information.

The safest way not to give away your personal information is not to generate it (leaving your phone and computer at home, or taking the battery out), but without going that far, we can instead choose much more privacy friendly software.

In particular it is preferable to use software 1) free/open source: whose content is verifiable in a transparent way by other people[7], 2) that sends messages readable only by the true recipient (using the so-called "end to end" encryption), 3) that minimizes the metadata that can be stored by third parties during use, 4) that does not rely on a single company (where the concentration of large amounts of data can attract the appetite of other companies or governments), but uses open and shared standards on decentralized networks. It is also useful to use long passwords and a password manager[1].