privacy

Tips on ****

A booklet for those who care about online security and privacy.

ONE OF US? SHOULD BE!

Brought to you by

tresorit

CONTENTS

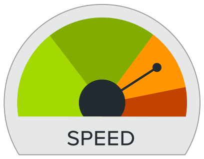
1 ANONYMOUS VPN

AND ANONYMITY NETWORKS

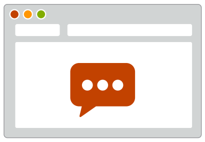
What does network traffic have to do with privacy? It might seem to be less privacy infringing at a first glance, but the truth is it can reveal sensitive information in many ways. If network traffic is not protected by encryption, anyone in between the communicating parties can learn whatever is being transferred. This is no surprise, as many of privacy conscious people use encryption to avoid being eavesdropped.

Does encryption solve all problems?

Many. But still a lot can be deduced:



by doing traffic analysis (e.g., inspecting traffic loads),



by monitoring who is communicating with who (e.g., learning user-website relationships),

or by observing timing of events (e.g., reconstructing daily/weekly schedule).

Is there anything else I should know about?

Definitely! Network mechanisms can be further exploited. Responses of the operating system to ping requests can be used to triangulate the location of someone within 690 metres. Since encryption is not hiding the IP address of the user, it can be used to determine location or to serve as auxiliary data for tracking. There is a great variety of tools available to tackle these problems, take a look at anonymity networks and network level anonymizers.

I'm not a security pro - what can I do?

No worries, all the of the following solutions are appropriate for beginners! One of the strongest classes of related solutions are anonymity networks. These include several solutions for hiding your IP address, and make traffic analysis harder for adversaries.

- *Tor and Jondo are the most widespread networks*
- *Both provide freely accessible services*
- *Find thier easy to understand descriptions on their respective websites*

As these protect only the traffic of applications configured to work with them, users who have higher demands can have their whole network traffic anonymized by using anonymous VPNs, such as ***Anonymizer****. Though network level anonymizers are strong privacy-enhancing technologies, all of them suffer a significant drawback: they offer protection only at the network level, while privacy violations can occur elsewhere, like within the web browser itself.*

2 WEB SURFING

Using an anonymity network like Tor alone, without the Tor Browser can be tracked easily by fingerprinting. If you are looking for a more complete protection, you should be using "readymade" solutions offered with these services.

Government surveillance makes up only half of the story, commercial surveillance also shows an emerging tendency. Collecting user (behavioral) data seems to be the new oil fueling many web companies and startups today. Why is this? Companies collect web user profiles for running personalized marketing campaigns, pursuing roughly the same business model as Facebook.

The most significant problems with this business model:

1. *lack of user consent*
2. *visibility of data collection*

Evidence shows that even if anonymous records are collected, such records can be re-identified leading to significant privacy issues. However, as the collection is anonymous, monitored webizens do not have chance to review, modify, or delete their data.

Is this a common practice?

Yes, unfortunately very common. Some *estimate* that there are watchers that can access more than 20% of our online digital activities. The same authors found more than 7000 tracker beacons within the Alexa top 500 in 2012, which belonged to more than 500 companies.

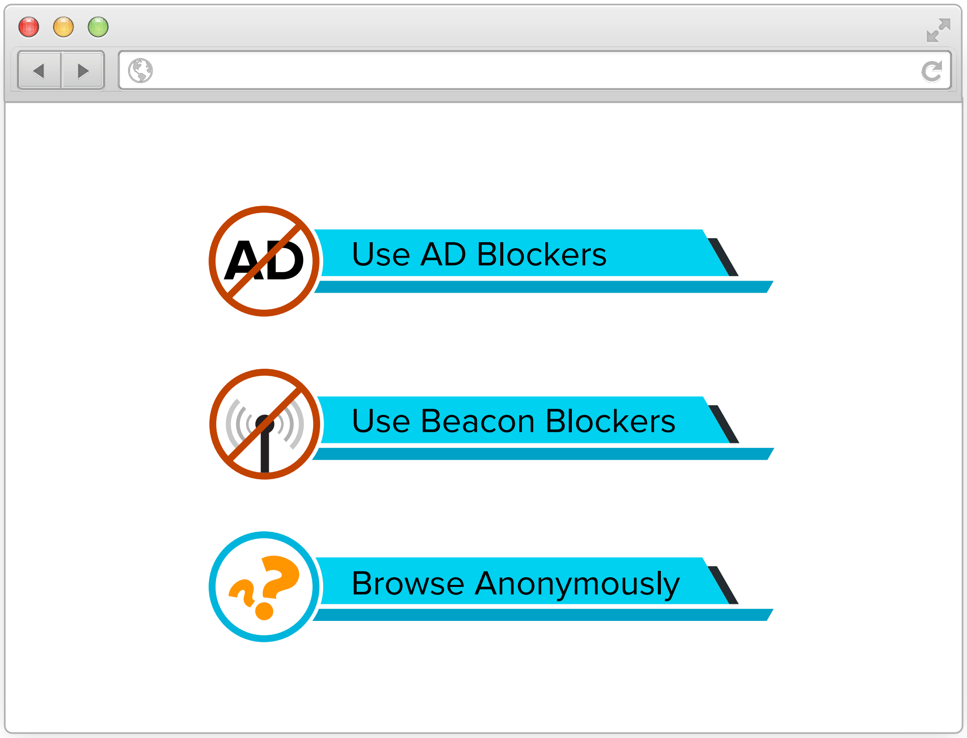
How is data collection done so covertly?

The whole technology is based on special kinds of beacons, called web bugs, unnoticeably embedded into websites. These act as a kind of CCTV cameras running a very precise algorithm, monitoring visitor movement in details. Whenever a user visits such a site, the web bug is triggered, and tries to identify the visitor. All stored activities are aligned to the user identity to provide further insights for trackers.

Identification is done within the fraction of a second, usually by reading an identifier previously stored on the visitors device (e.g., in the form of tracking cookies or other storages), or by identifying the user device by its fingerprint.

This sounds technically even more complex. Is there a way for opting-out?

There are pretty good lightweight solutions on the market, like beacon blockers (e.g., Ghostery) and ad-blockers (e.g., Adblock Plus). If you are willing to sacrifice some convenience, use anonymous browsers, like the Tor Browser Bundle or JondoFox. These are developed by some of the best security professionals out there, and are preset to use network level anonymizers and tailored to protect against most known privacy issues.



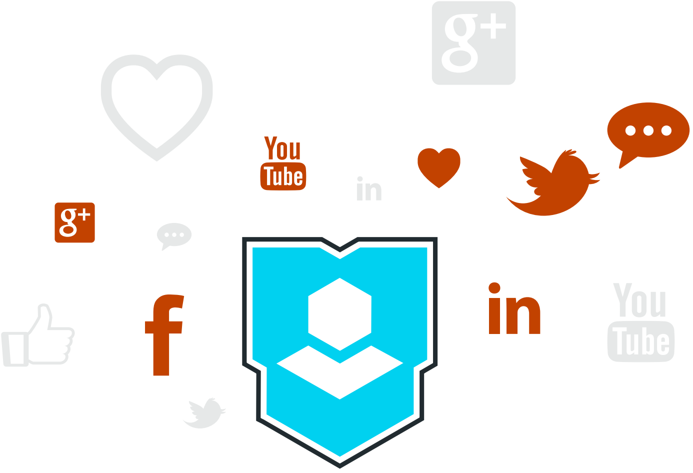
3 THE INTERACTIVE WEB:

SOCIAL NETWORKS, COLLABORATIONS AND PUBLICATIONS

Surveillance is not the only source of trouble to think of. Our social activities also reveal a lot: who we meet, when and where, what we like on Facebook or retweet on Twitter, the pictures we share, the content we publish on our blog. Sure, we do them to have fun, socialize, and so on. However, there are some secondary "uses" to think of: internet technology brought Big Brother closer and gave birth to 'little brothers'.

Little brothers?

Technology made gathering information on individuals or even masses of people a lot easier, making carrying out espionage feasible for basically anyone. These little brothers can be your friends, or your future employee, checking out your records, what you "liked" on the web, what posts or photos you've been uploading. In fact, a potential employer or new acquiantance can learn a lot by looking behind the scenes, and analyzing your social activities.



So it's better to think twice before trusting any personal information to the web – as the core of the problem is with the lack of future control of your information. It can be impossible, or at least very hard to remove or modify something once submitted. With the emergence of real time searches (and archiving sites), revocation is even harder. Today, we're just seeing the tip of this problem's iceberg, but the upward trend of putting our personal data out there will have a huge impact on privacy. We won't be able to change our identities anytime we want.

So should I flee from social media?

Nope, no one would ask you to do that. Rather, be rational – consider your actions and their implications is the best you can do. This is as simple as it sounds: regain control over your data by thinking things over before uploading, sharing, posting.

Be a conscious consumer:

CHECK YOUR PRIVACY SETTINGS

CONTROL THE VISIBILITY OF YOUR ONLINE IDENTITY

set up different access levels

You can do that on many platforms by creating lists and groups.

encrypt libraries embedded into your blog

e.g. jsencryption for advanced users or you can use some easy-to-use encryption plugins like ***CryptFire*** *or encrypted* ***communication.***

4 MANAGE YOUR ONLINE IDENTITIES:

HIDE FROM INFORMATION SUPERPOWERS

Still not satisfied? Take your privacy's protection to the next level.

Not everything is about what you use. You may also consider having multiple social network registrations (i.e., multiple online identities) to make monitoring of your actions even harder. Consider running a blog in a sensitive topic (eg. politics, religion, restaurant reviews,) under a different name, linked to a Facebook registration created for blogging purpose in order to avoid future conflicts. It is up to you to decide if you need it or not – most people living in democracies probably would not need such preventive measures.

case study

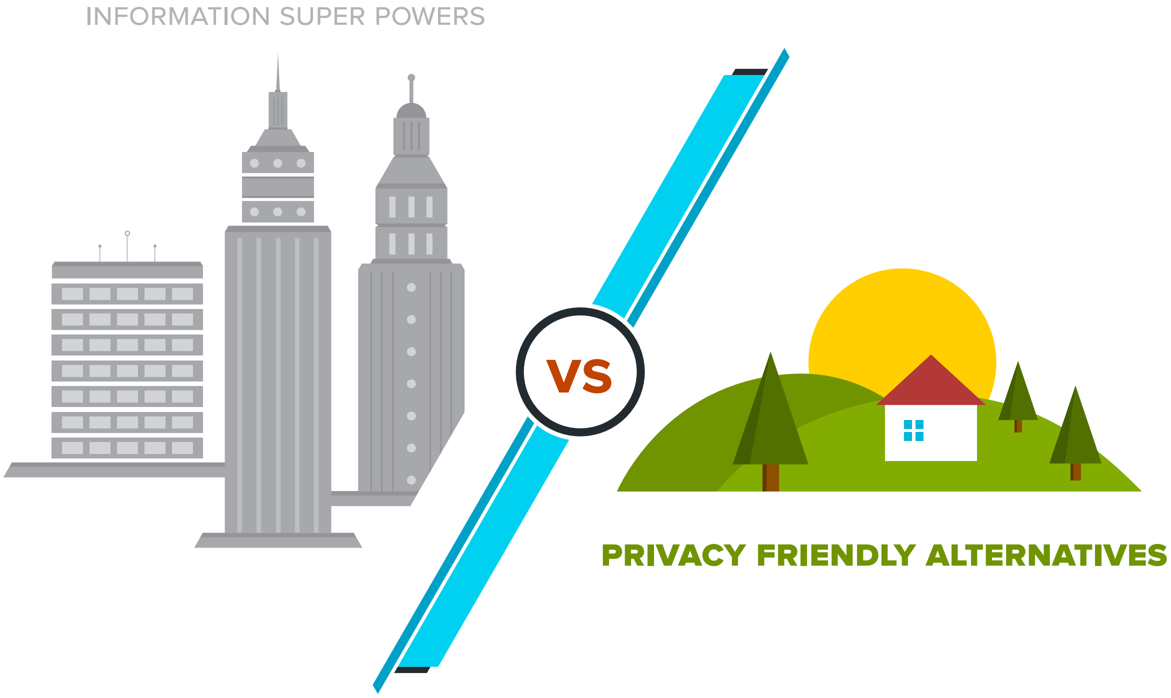
The Netflix-case gives a perfect example how single identities can compromise privacy if our data gets out, even anonymously. Let us consider someone posting movie ratings and reviews to IMDb under his real name, rating the similar films anonymously on Netflix pages. Even some movies that our subject would otherwise not share with friends or colleagues (e.g., because of sexual or religious content).

*However, **scientists showed** public IMDb records can identity 99% of users in the anonymized dataset, meaning that even ratings that were thought to be private can be aligned to their names. The underlying principles of this problem is very general, and thus in similar cases, using multiple identities (with precaution) should be concerned.*

Big data, big money: information superpowers

Online service providers offering a wide-scale portfolio found a business opportunity in building vast datasets of their users (for which the most famous examples are Google and Facebook). If someone is using several of their products, they can get even more from your personal data. No need to give up convenience or privacy – but make sure to be more concious! Don’t rely exclusively on products of the same vendor. Take a step forward and use more privacy friendly or open source alternatives for different purposes.

Make sure to check your privacy settings! Usually because of advertising reasons service providers treat almost everything as "public" by default. This way individual user posts are more visible web-wide, ads are better targeted, and potential reach of paid advertising is maximized.



5 EMAIL PRIVACY

Email privacy has a lot of issues.

1. Hide the content of your emails via encryption

   Note: webmail can even reveal your IP address

2. Consider hiding meta-information of your communication:

   who you communicated with, when, about what topic, and so on. If this information would not be important, it would not be retained in the European Union, and would not be collected by the NSA. To cover your metadata, choose an email service provider that falls outside the reach of relevant authorities. The best way is to use anonymous remailers for the sensitive part of your communication.

3. Always be wary of images in emails

   Web bugged emails can also leak information – this is why newsletters often contain images: to make measuring detailed user actions possible.

Know that someone can leak your email address. Disposable email addresses can mitigate this easily, as you can use them until you decide otherwise: even for only a few hours or a few occasions, and then easily cut the messaging chain.
If you insist on using a permanent address of your own, you can also add an alias to the address (e.g., dr.john.doe+myemail@gmail.com) at each site where you use it – if it gets out, it is easier to redirect the traffic to the spam bucket.

6 PROTECTION OF YOUR FILES

Prying eyes of governments (or even business competitors) are often seeking ways to access your files for analysis. But the risk is even more complex: you may lose your laptop, and all your personal files, such as photos, emails, passwords and corporate secrets along with it. Let's see how you can prepare for these situations!

Use encryption

Backup your files

Build your local personal file safe

Your laptop and external drives can be seized at the airport, or while crossing borders. To protect personal files and company secrets you can put these onto an encrypted drive, as there are several alternatives to choose from.

- *Try **TrueCrypt!** It also provides plausible deniability, which means that you can create hidden drives whose existence can be plausibly denied. However, TrueCrypt has recently been criticized and **lost some credibility,** as its authors are practically unknown and while its source code is public, it was not reviewed as thoroughly as possible.*
- *Encrypt files before you transmit them.*
  When you send them in email or via instant messaging software, they are vulnerable to eavesdropping. In order to avoid that, share them by using encryption technologies ensuring that they can be only accessed by the intended recipients.
- *Backup your files.*
- *Minimize your casualties in case you lose your laptop or some files due to system failures (encrypted stuff can be harder to repair) by using backup systems. Easy to use backup software is now a mandatory part of modern operation systems, such as Time Machine in OSX, or File History in Windows 8. For older operating systems, there are similar solutions such as **Genie Timeline,** and you can also find solutions storing backup files in the cloud, like **Tresorit.***

protect your file's privacy in the cloud

tresorit

Tresorit is a cloud-based file share and backup service designed to prevent eavesdropping on shared and transmitted data, as not even the company's servers can access your privately stored content.

	TRESORIT	DROPBOX	BOX	GOOGLE DRIVE	WUALA
Sync any folder	✓	✗	✗	✗	✓
Share encrypted content	✓	✗	✗	✗	✓
Easy install, no admin required	✓	✗	✗	✗	✗
Folder and user level, granular permissions	✓	LIMITED	✓	LIMITED	✓
Client side encryption with AES-256	✓	✗	✗	✗	✓
Server cannot access stored data	✓	✗	✗	✗	✓
Non-convergent crypto	✓	✗	✗	✗	✗
Sharing is encrypted	✓	✗	✗	✗	✓
ISO27001 and SSAE 16 certified datacenters	✓	✗	✓	✓	✓

7 SECURING ONLINE PAYMENTS

The worse nightmare of anyone using an online payment method is the provider getting hacked: besides the loss of your privacy (e.g., your purchase history is revealed), you may easily face financial losses, too.

Your credit card number (with other personally identifying information) can be stolen, and can be used for unwanted charges and fraud – limiting and controlling such usage is hard. There are cases when you may want to remain anonymous when buying, or paying for a service. In other words, you do not want your actions being linked to your person or earlier spendings.

Is there a way to protect myself from these issues?

There are two types of products to overcome these problems: pseudonymous cards and solutions provided for single transactions. Some banks offer alternative, internet-based (or even disposable) bank cards for online payment, and there are companies also offering such solutions. Products providing transactional usage offer even more privacy.

- *Albine offers MaskMe, a web browser extension capable of generating temporary bank cards when you're in the middle of the check-out, and filling out the buyer details.*

- *Pre-paid paysafecards can be bought offline, and can be used up to their nominal values, for instance, to buy premium rates for browsing anonymously.*

8 PASSWORD MANAGEMENT AND MORE

Password management without post-it notes

Password management is usually considered an annoying side issue, but it is extremely important: your passwords are the keys to your online persona. Recent Adobe password leaks shed light on how many people use weak passwords, even when there is plenty of advice available for choosing good passwords. The problem is that we cannot remember dozens or even hundreds of unique, strong passwords.

This is where password safes come into action. These applications can store passwords in encrypted offline databases, and automatically type them in when needed – they can even operate outside the browser! PasswordSafe and KeePass are two well known names. Both have iOS and Android apps too, so you can take your passwords with you wherever you go.

Camouflage on open ground – professional solutions

Under specific circumstances (e.g., using a public computer during holidays) you may need special pre-set solutions for accessing the internet, without leaving any traces of your data or identity. For such cases, there are tails and JonDo Live-CD, including complete operating systems that can be used securely and privately for communications and more.

For topics not covered above, feel free to look around for the solution you need! As a starter, check out one of the repositories on privacy-enhancing technologies, like the EPIC Privacy tools or Shadow Tracer' kit.

tresorit

Professional content written by Gábor Gulyás