# Introduction

It is a common misconception that you can't stop the government from spying on you. You can. Don't let fear of government crackdown prevent you from voicing your opinions. The Ritser Privacy Toolkit is designed to help keep you safe and informed.

# How the internet works

All computers on the internet have an IP address that they use to communicate with each other. Websites also have IP addresses, but to make internet browsing easier, they also have domain names (such as www.facebook.com and www.google.com) that are linked to their IP addresses. When your computer wants to go to www.google.com to perform a search, it gets the IP associated with it and communicates with that computer to obtain the information, in this case your Google search results.

Your ISP (internet service provider) is what connects your computer to the internet. You probably have a modem that is connected to the ISP's network using a telephone, television, or fiber optic cable. Because your internet passes through their infrastructure, they can see all the data that you transmit and which IP addresses you are sending information to.


But this doesn't mean they have to know which web pages you are visiting. If you encrypt your data using HTTPS or Tor, they won't see what's going through, including the URL (www.google.com/search?q=news). They will only know the IP address you are connecting to, the time you are connecting, and the size of the encrypted data you are sending.

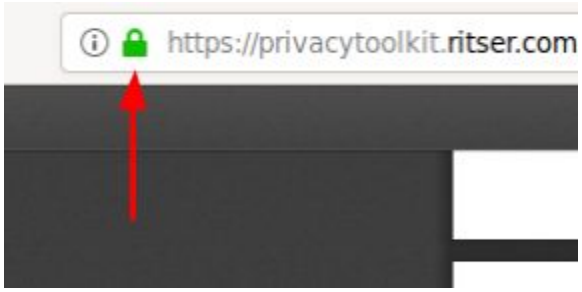
# What the government can already track

Let's go over what the government/ISP can track. Assuming you're using HTTPS but not Tor, your government can track which websites you're using and when. This means that they will be

able to know you accessed the IP address of www.facebook.com at 7:38 PM, but they won't know what pages or profiles you visited. They'll only know you visited www.facebook.com.

If you're *not* using HTTPS, your government will also be able to track what you send to the website. This includes passwords and URLs.

How do you know if you're using HTTPS? Well, usually, your browser will display a lock symbol as shown below when you're browsing using HTTPS.




HTTPS works by encrypting the data between your browser and the website. This means that it uses mathematical algorithms to make sure that this data is unreadable while it is in transit. Modern encryption algorithms are considered to be secure, as even the most powerful intelligence agencies are unable to break them.

Unencrypted connections (HTTP without the S) look like this:

**From:** 70.210.154.182

**To:** 103.190.246.203 (baidu.com)

**Time:** 4:42 AM 2020-09-02

**Data (70 bytes):**

Webpage visited: baidu.com/account

Username: alex2

Password: password

Encrypted connections (HTTPS) look like this:

**From:** 70.210.154.182

**To:** 103.190.246.203 (baidu.com)

**Time:** 4:42 AM today

**Data (68 bytes):**

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

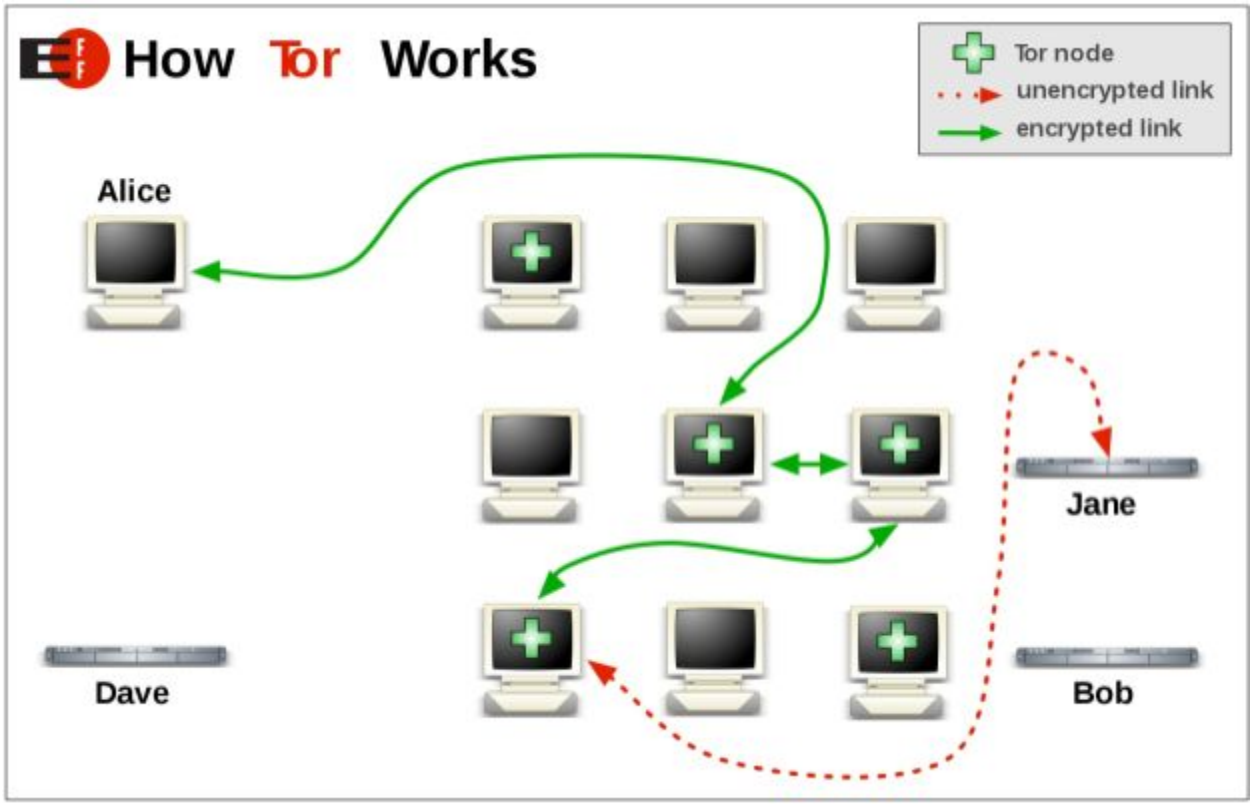
## What the government can track with the help of website owners

However, HTTPS does **not** prevent the website from giving your data to the police. Every single website you access on the internet can see your IP address. If a website decides to give the government the IP address behind your account, **they can use it to find your real address.** It's important to make sure that the authorities cannot find the IP address behind your online accounts.

Big websites such as Facebook, Reddit, and Google have procedures in place to handle government requests for user data. This process is usually somewhat transparent and fair, as they generally ignore laws of authoritarian governments. Google, for example, processed 3 Egyptian user data requests between 2014 and 2018. They denied all of them.

## Hiding your identity from websites

However, it's not a smart idea to put your safety in the hands of multinational for-profit corporations. If you live in a country where your safety is at risk if your identity is revealed, it's a good idea to use Tor (included in this toolkit). Tor hides your IP address by sending your internet traffic through other computers before it gets to the website. The website will be able to see the IP of the last computer instead of yours. Your government will know that you're accessing Tor, but they won't know what you're sending through it or who you're communicating with.




Another benefit of using Tor is that since the ISP doesn't know which websites you are accessing, they can't block them.

Tor isn't infallible. If the government knows your approximate location and the website owner tells them that you're using Tor, they can check who accessed Tor at that place at the same time you viewed the website to obtain your real identity. The FBI has done this before, but it should rarely be an issue. If you're concerned about this, you can use public WiFi.

**Side note:** VPNs aren't as effective as Tor at keeping you anonymous online.

## The obvious

What usually gets people caught isn't that the government obtains their IP address. It's that they submit something to the internet that reveals their identity or reveal their identity to their friend. Dumb mistakes are what get people caught. Here are a few examples of things you should always do:

1. When submitting stories, be vague and make up details. A small piece of information, such as the number of siblings you have, can be used to uncover your identity.
2. Be **very** careful when submitting photos to the internet. Scrub EXIF data from all photos you upload and verify that there are no details that may be used to identify you.

3. If other people use your computer, make sure your browsing history isn't saved. Don't save anything to your computer that may give away your identity.
4. Don't use your real name to sign up for the accounts you use for your anonymous identity.
5. Don't reveal your anonymous identity to people you know in real life.
6. Don't reveal your real identity to people you know through your anonymous identity.

# Conclusion

If you make anonymous Reddit or Facebook accounts, you can sometimes stay safe. But you may not want to trust these companies if your life depends on it. If you want to confidently stay anonymous, use Tor. PrivacyTools is a good resource for other privacy-oriented software.

And remember: Only you are responsible for your own safety.