

# Guide for Online Privacy and Anonymity: Activist Tools and Security



By [Fred](#)

How can you keep your anonymity, online privacy and personal security safe? If you are an activist or whistle-blower, your security might be at stake now. If you are just a normal internet user, you are been shown advertisements and tracked every page you visit.

Online privacy is a very important and crucial requirement for any activist. It gives you protection and anonymity from corrupt government agencies, such as the US Government, CIA, NSA, social networking sites, Twitter, Facebook, Yahoo! Mail, Google Mail (Gmail) and Skype.

Social networking sites can and do provide the government everything about you when they are asked. For example, all of your IPs ever used, your geo location (from geopip or a html5 feature in your browser), timestamps of your activities, your full profile information and everything else about you that can be used to put you in jail for exposing the truth or blowing the whistle on some powerful people.

Yahoo! Mail and Gmail also have the records of providing the government with your login information, together with all your emails. There was even a PDF with procedures for the police leaked from Yahoo!:  
[Compliance Guide For Law Enforcement](#)

Another example of social networking providing user information to the government was the case of Birgitta Jónsdóttir, an active activist and member of the Icelandic Parliament, accused by the FBI of having connections with Wikileaks.

Twitter provided the FBI with her IP addresses and times of login. The FBI tried to go to Iceland to investigate Wikileaks and possible Birgitta connections, but the Icelandic authorities kicked the investigators out and banned them from ever returning to Iceland.

<https://worldmathaba.net/items/2322-fbi-banned-from-iceland>

This compliance guide is designed to assist law enforcement in understanding Yahoo!'s policies and practices with regard to retention and disclosure of electronic information and to provide answers to frequently asked questions related to subpoenas, and other legal process.

....

What Information Can Yahoo! Provide?

Subscriber Information:

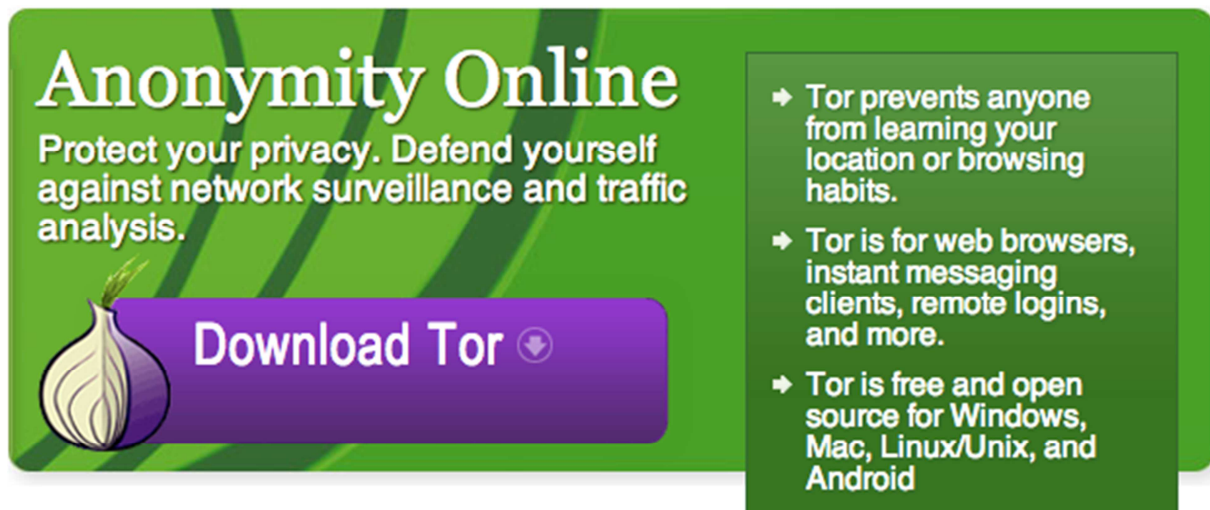
- Subscriber information supplied by the user at the time of registration, including name, location, date account created, and services used.
- IP addresses associated with log-ins to a user account are available for up to one year.
- Registration IP address data available for IDs registered since 1999.

...

## What can you do to keep your privacy and anonymity?

Here is a list of software applications that you can use to accomplish total anonymity and privacy:

### 1. Tor



The banner features a green background with a purple button that says "Download Tor" and a small onion icon. To the right, a list of three bullet points describes Tor's benefits.

**Anonymity Online**  
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

**Download Tor** ↓

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Tor is considered the best tool for activists, it completely hides your location since your IP is not visible. From Tor website:

### What is Tor?

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as [traffic analysis](#).

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Tor encrypts your traffic too, protecting your data from being monitored and captured by your ISP, hackers on your network, your work network, and anyone on the same Local Area Network.

<https://www.torproject.org/download/download-easy.html.en>

## 2. PGP

[PGP](#) is a standard for general encryption. Tools such as GnuPG allow to encrypt and sign your data and communication such as emails, text files, images, and anything you believe is private and should not be seen by anyone else except the destination user.

From Wikipedia:

**Pretty Good Privacy (PGP)** is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.

Here is an example of an encrypted email: (some parts were omitted because they were too large)

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.9 (GNU/Linux)

hQIOA25r3V3Gbvc4EAF/W8bDfIefuL5tAKkxLierBTywvBM+ilIWQeTxQS6bA9QM
CTt7lomrIjdVyXVpiRds0+y2MPG0lq7Cf45BFc1MTsh06s4lq+prQpMKER2tZXXS
o7Vril8rX75gNjLWOLOWsRVPVe3gyqwgimdiqDeQblr0bVj4+FBqqdRH4M4U0zGJ
tkDKlFmud4YeLAvpyxhm8LXpfSatD168d5gxMHitIFdAztWp4BWxKVclrGPq5s99
PILcHd/l4QsyjUGTI1UujJkOPF/C77EU4xBFqOfYTub8sXBLw+4eH96sEfhqAxmS
FywkLqJbLPTyGtZzD3lz30zQz/grfpO+LkBUGd14g+Qen/Rdq4ziD/0usoBMXN8
23XRNDogwHTowgxOfwrMDEq8RA8E2+5YCjMTE/BY9PZfVb0LangcKiHaqSb3QzDZ
3oKHssHg+zhF2RbcXvAYZFG2GK9bJrk9PeFhoN2TZfJcF58kqC8H0w0PZcdNa1Nq
. . . .
KBj1jGmBC85817/E7eBn0UgobuGyu8rCtT6QlDBX3wO/Rm211+cXVxXoUON8X8p
Y9pBm1p5rUnLGe7y+sFnOc+imxXUxQgl0pyjqBswtw5vwC+mGUo24PXqS91d0dC
N1RtvK6gk4a65Ng7sRTXS/dlwk/7IddXk3vFyUzoa/CuKZ2IAUknwyN+1QuKnvSM
gOp2dgxsAsywOJp1DV9qEmRhOHNFfxkSGN7di9SX1UPATOely1BjVJVPVgQc j3yZ
u8V7/4DsFDt9MuXq0sC5tVRGqLAZxnI4KMLJBr+ftL8NOS3SDPHJpdvjVqJj6oSW
P3LI9bGuYI6pcb/jIp+AI49BFU7uFyz86vUUzftCpYkBO6m/5RTU1zaNH5ZJZCQJ
R0x3GVRhWnD0p78ASqBGAU8BA1z4o+Oq5vgVeDKrC15V4bYzXlztUi4m1nZ6LIC9
I/FSQWnYdK7jNWLWuzQ9ps8/uFzMaU+mHLR56rPN2fvuLOVaz0uxYAoAJ8fm7iRG
SWTMstttTCP+Rj50823z4z2PL7ABUM24SYGVjen1r/ay9SCI
=4K9D
-----END PGP MESSAGE-----
```

As you can see above, the email is in no-readable form (encrypted). Nobody can read the email except the destination person who you encrypt the email for. This encrypting scheme is extremely strong, I highly recommend it to be used on a daily basis for email and file transfers.

Complete ready to use tools are available for Mac OS X, Windows, Linux.

For Mac: <https://www.gpgtools.org/>  
Windows: <http://www.gpg4win.org/>  
Linux: Use your Linux package management.

### 3. OTR: Off-the-Record Messaging

[Off-the-Record Messaging](#), commonly referred to as OTR, is a cryptographic protocol that provides strong encryption for instant messaging conversations. OTR uses a combination of the AES symmetric-key algorithm, the Diffie–Hellman key exchange, and the SHA-1 hash function. In addition to authentication and encryption, OTR provides perfect forward secrecy and malleable encryption.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- Encryption: No one else can read your instant messages.
- Authentication: You are assured the correspondent is who you think it is.
- Deniability: The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- Perfect forward secrecy: If you lose control of your private keys, no previous conversation is compromised.

### 4. VPN

A VPN (Virtual Private Network) can also be used to encrypt your internet traffic, to bypass internet censorship and partial anonymity.

In a VPN your internet traffic is completely encrypted, however you will always have the same IP, which is the server IP of your VPN. Using a VPN is better than using proxies, but not as good as TOR.

There are free and paid VPN services available, you can also build your own VPN using a Virtual private server and OpenVPN (VPS + openVPN). OpenVPN is an SSL based VPN and easy to install and configure.

For example, a cheap Amazon EC2 micro instance (VPS) can be used for VPN and the cost can be between \$8 and \$16/month.

### 5. Proxies

Public Proxies (or paid) can be used as a last resort when you need to have anonymity. Proxies provide partial anonymity, but they are not safe and trusted. They can be compromised or even be owned by government agencies.

The main purpose of proxies are to hide your IP, nothing more. It does not provide secrecy and protection as Tor or VPN. Also note that you traffic through a proxy is un-encrypted, thus you should avoid using Proxies.

## **6. You phone numbers**

Never give your phone numbers to social sites and email providers.

By now your phone numbers should already be on your Facebook, Gmail, Yahoo! and Twitter profiles.

Google Mail, Facebook, Yahoo! and most social media sites are always asking you to provide your phone number(s) and usually give warnings for you to update and insert your phone number if you haven't yet. Those messages are annoying and in the end the user will just provide the number so that the annoying messages on the screen can go away... well, don't do that!

Giving your phone number is like giving them a GPS tracker on you! With the help of your local government and police (not all countries), they can track you everywhere you go using your cell phone tracking abilities which you "cannot disable". Facebook makes it almost mandatory to have a phone number which "validated with an SMS" in local language for the country it belongs to. You can't use many Facebook features if you don't provide your phone number. In that case if you really have to do it, then you could try using a one-time SIM card and throw it away after, or someone phone you have little connections with.

Google Mail and Yahoo! also make it very important that you provide your phone number. You should not have to provide it, if so you can provide a random number.

## **7. Facebook on Android phone**

Facebook on Android will have access to your address-book and upload to Facebook everyone on your phone list, including phone numbers and emails. You can see all permissions that Facebook has on your Android phone here:

<https://play.google.com/store/apps/details?id=com.facebook.katana>

When you install Facebook on your phone, it will ask to "synchronize" your phone contacts with Facebook, which in fact it will upload your contacts database to Facebook, now Facebook knows all the phone numbers and emails of everyone on your phone! Isn't that scary?

Some of the Facebook special permissions on your phone and tablet: (only named the most important)

- TAKE PICTURES AND VIDEOS (take videos and pictures WITHOUT you knowing it's happening)
- YOUR LOCATION: APPROXIMATE LOCATION (NETWORK-BASED) and PRECISE LOCATION (GPS AND NETWORK-BASED)
- FULL NETWORK ACCESS

- READ YOUR CONTACTS
- MODIFY YOUR CONTACTS
- PHONE CALLS (see your phone calls)
- READ PHONE STATUS AND IDENTITY (read your actual phone number)
- MODIFY OR DELETE THE CONTENTS OF YOUR USB STORAGE MODIFY OR DELETE THE CONTENTS OF YOUR SD CARD
- PREVENT TABLET FROM SLEEPING PREVENT PHONE FROM SLEEPING (keep your phone/tablet awake and control it's hardware)
- TOGGLE SYNC ON AND OFF
- FIND ACCOUNTS ON THE DEVICE (see accounts created from other applications)
- VIEW WI-FI CONNECTIONS (here Facebook can see the WiFi access points near you)
- VIEW NETWORK CONNECTIONS (view information about network connections such as which networks exist and are connected)
- WRITE CALL LOG (modify your call records)
- READ CALL LOG

These exaggerated permissions are not only common to Facebook, but also used on other apps such as Twitter.

Facebook on Android can be used as a powerful spy tool, be aware.

## **8. Password protect and encrypt your phone**

Always put a password on all your mobile phones and computers. If you don't want the police to search your phone without a warrant, make sure it's password protected. In Canada, a court ruled that police can search unprotected cellphone without warrant. ([source](#))

Make sure the password is long and not your birthday, postcode or last name. On iPhone use a pass-phrase, it's longer and much harder to guess. Android does better with password protection, it allows you to use patterns which are hard to crack.

Use updated version of iOS on your iPhone, several iOS version have bugs that allows anyone to bypass the screen-lock and enter your phone, namely, iOS version 6.0, recently released. Update to iOS 6.0.1 immediately.

Some Android phones can still be accessed and bypass your password protection by "rooting" it. A process that removes the superuser protection on the phone and allows data extraction. But it can be remedied by encrypting the whole phone and using a tool called SuperSU that prevents un-authorized root access to your phone.

How to encrypt an Android phone:

<http://support.google.com/android/bin/answer.py?hl=en&answer=1663755>

Blackberry phones are still the harder nut to crack. They are encrypted and cannot be bypassed by exploits, the most secure available.

## 9. Firefox/Chrome privacy modes.

Firefox Private browsing mode and Chrome incognito mode gives you an extra privacy by not storing tracking cookies, browsing history or login sessions, so when you open the browser again you will start fresh. It does not completely protect you, but it does help on some occasions. Google Chrome incognito description:

You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close all open incognito windows. Any files you download or bookmarks you create will be preserved, however.

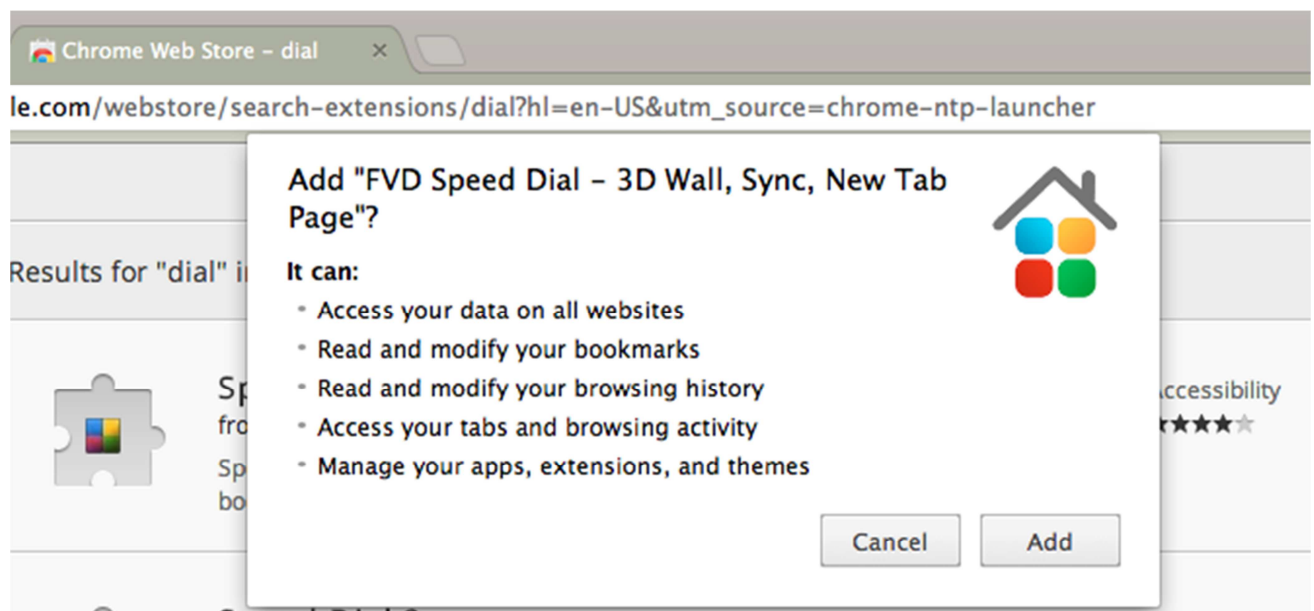
## 10. Use updated and modern browsers

Keep updated your browsers: Firefox, Chrome and Opera. Avoid using Internet Explorer due to its security weakness.

## 11. Don't install browser extensions you don't really need

Browser extensions also have access to your bookmarks, website data, history, and other data that should never leave your computer. Only install the necessary and trusted browser extensions.

Chrome extensions permissions screenshots:



## Recommended Browser extensions for privacy and anonymity



**DoNotTrackMe:** It protects your privacy by blocking online tracking. Every time you use the web, companies are collecting and storing info about you and your web activity. DoNotTrackMe (DNTMe) is free privacy software that prevents online tracking and improves your security on the Internet.

Google Chrome:

<https://chrome.google.com/webstore/detail/donottrackme/epanfjkhahimkgomniadpkobaefekcd>

Firefox: <https://addons.mozilla.org/en-US/firefox/addon/donottrackplus/>

**AdBlock Plus:** It Blocks all annoying ads on the web: video ads on YouTube, Facebook ads, banners, pornographic ads and much more. Enjoy surfing the web without obtrusive ads cluttering your screen.

Google Chrome: <https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnlbpkdaibdcccddilifddb>

Firefox: <https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/>

**LastPass:** The most secure password manager on the Internet. Do you trust Google and Firefox Password managers? <https://lastpass.com/>

**WorldMathaba Firefox addons collection:** We have created a collection of add-ons for Firefox for privacy and anonymity: <https://addons.mozilla.org/en-US/firefox/collections/worldmathaba/anon/>

## **Android Privacy for the advanced users and hackers**

A new project called [OpenPdroid](#) aims in providing full control of permissions on the Android operating system.

*"OpenPDroid is a set of modifications to the Android framework and libraries which allows fine-tuning of the data which applications are able to retrieve about your device, your account, your messages, and more. Specifically, it is a Privacy service provider (using the PDroid 1.51 interface) forked from [CollegeDev's PDroid 2.0](#), which is itself an extension of [Syvat's PDroid](#)."*

In order to have OpenPdroid installed you need to have a rooted Android device. You will have to create a CWM zip file on your own from your ROM original zip file (the zip file you flashed on CWM). Once your ROM is patched to used OpenPdroid you will need [OpenPdroid Manager](#) to configure the permissions.





*A screenshot of OpenPdnoid Manager settings for Skype*

As you see above, I have disabled Skype permission to see the people I have called, the complete call history, ability to record audio from the microphone, ability to get my WiFi access point name (can be used for tracking location), and my contacts from address book.

I even went as far as proving Skype with a modified GPS coordinates. I provided Lat: 0.0 and Lng: 0.0 (for Skype, I'm in the middle of the Atlantic Ocean) see Network location.

With the above settings Skype does function properly.

Any suggestions, recommendations or critics, are welcome to be left in a comment below.

*Update: Added paragraph "8. Password protect and encrypt your phone"*

