Windows

Warning: Microsoft Windows is affected by PRISM. Even using the software tools we recommend here, your privacy may be compromised by Windows. The operating system of any device can unfortunately lever out any privacy protection that a program tries to offer you. The latter has to run in the confines of the OS after all. We strongly recommend replacing Windows with either Linux or BSD.

Anonymizing Networks

Prefer		✓

I2P
The invisible internet project.   ↗

Tor
Free software for enabling online anonymity. Tor directs Internet traffic through a free, worldwide, vo…   ↗

Bookmark Sync

Prefer		✓

wallabag
wallabag is a self hostable application for saving web pages. Unlike other services, wallabag is free…   ↗

Avoid		✕

I Instapaper

Pocket

Collaboration

Prefer		✓

Cryptpad
Real-time collaborative docs, polls, todos.
Web Service   ↗

Loomio
Web application that helps groups of people to make decisions together.
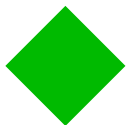Web Service

DNS

Prefer ✓

dnscrypt-proxy ↗
Encrypted DNS proxy.

Namecoin ↗
Distributed DNS for .bit TLD.

nsupdate.info ↗
Dynamic DNS service.
Web Service

Avoid ✗

Google Public DNS

OpenDNS

Email

Prefer ✓

Kolab Now ↗
Kolab accounts hosted in Switzerland.
Web Service

Riseup ↗
Secure communication tools for people working on liberatory social change.
Web Service

Thunderbird ↗
Extensible, cross-platform email client.

Notes

For more email providers, take a look at Privacy-Conscious Email Services. Please decide for yourself whether if you trust them with your data. For more discussion about safe email providers, please see issue #461.

MyKolab is hosted in Switzerland and benefits from the strong Swiss privacy laws. It is run exclusively with free software and using the service supports the development of **Kolab**. Also, it lets you export all your data at any time.

Riseup's services may also be accessed via their Tor Hidden Service addresses. A list is available here.

Why not Hushmail? See 'compromises to email privacy'.

If you have the technical aptitude, consider running your own mail server.

Avoid	✖
Gmail	
GroupWise	
Microsoft Outlook	
Yahoo Mail	
Yandex.Mail	

Email Addons

Prefer	✔
Enigmail OpenPGP add-on for Thunderbird.	↗
Mailvelope OpenPGP browser add-on for webmail.	↗
TorBirdy Tor add-on for Thunderbird.	↗

Notes

"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."

— Wikipedia

PRISM Break does not recommended S/MIME email encryption because of its reliance on third-party certificates from central authorities. Read more here.

OpenKeychain together with **K-9 Mail** provides end-to-end email encryption. An experimental project is GnuPG for Android by the Guardian Project.

Read the Email Self-Defense guide by the Free Software Foundation to learn how to encrypt your email messages.

Enterprise Suite

Prefer	✓

Nextcloud
A safe home for all your data ↗

Sandstorm
Sandboxed platform for self-hosting web apps. ↗
Web Service

Notes

The enterprise suite category is for solutions for organizations that cover more than 10 categories in an integrated fashion (ex.: logins work throughout all apps, etc.)

Avoid	✕

G Suite

Office 365

Zoho Office Suite

File Sharing

Prefer	✓

OnionShare
Anonymous file transfer via Tor. ↗

Up1
Client-side encrypted image host web server. ↗

File Storage & Sync

Prefer	✓

Cryptomator
Client-side encryption for cloud storage. ↗

EteSync
Journaled calendar and contacts sync. ↗
Web Service

git-annex
Git-driven file management and version control.

Gridsync
User-friendly sync with Tahoe-LAFS grids.

Experimental

Least Authority S4
Unlimited S3-backed Tahoe-LAFS grid.

Web Service Experimental

Sia
Decentralized cloud storage.

Experimental

Syncthing
Direct file sync between devices.

Notes

This section has been carefully curated to only include software that encrypts data on the client. That means your data should be secure even if servers it's stored on are compromised.

Avoid

Dropbox

Google Drive

iCloud

Microsoft OneDrive

Yandex.Disk

Finance

Prefer

Bisq
Decentralized Bitcoin exchange.

Monero
Fungible, untraceable cryptocurrency.

Avoid

PayPal

Instant Messaging

Prefer

Psi
Cross-platform XMPP client.

RetroShare
Peer-to-peer communication and file sharing app.

Signal
Metadata-resistant, user-friendly messenger with audio/video calls (mobile only).

Avoid

Discord

Facebook Messenger

Google Hangouts

ICQ

LINE

Skype

Snapchat

Tencent QQ

Trillian

Viber Messenger

WeChat

Media Publishing

Prefer

PageKite
Localhost tunneling service.

Web Service

PeerTube
Federated video hosting.

Web Service **Experimental**

PixelFed
Federated image sharing.

Web Service **Experimental**

WriteFreely
Federated blog platform.

Web Service **Experimental**

Avoid

flickr Flickr

Imgur

Instagram

Medium

Tumblr

Vimeo

YouTube

Mesh Networks

Prefer

Cjdns
A networking protocol, a system of digital rules for message exchange between computers. "Instea…

tinc
Free software daemon that uses tunnelling and encryption to create a secure private network

Notes

A mesh network is a decentralized peer-to-peer network, with user-controlled physical links that are usually wireless.
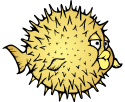
"Mesh networking (topology) is a type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes, that is, it must collaborate to propagate the data in the network."

— Wikipedia

News

Tiny Tiny RSS
RSS feed reader.
Web Service

Google News

Operating Systems

Debian
Popular ethical GNU/Linux distribution.

Fedora
Fast, stable and powerful GNU/Linux distribution.

FreeBSD
A free BSD-derived operating system.

OpenBSD
A secure BSD operating system.

Qubes
Fedora/Xen-based OS designed to provide strong security through isolation.

Notes

Apple, Google, and Microsoft are allegedly a part of PRISM. Their proprietary operating systems cannot be trusted to safeguard your personal information from the NSA. We have two free alternatives: **GNU/Linux** and **BSD**.

GNU/Linux has a much larger community to help you with the transition. It's recommended that you begin your explorations by looking for a GNU/Linux distribution that suits your needs. Additionally the Free Software Foundation hosts a list of completely Free distributions.

Debian has a long tradition of software freedom. Contributors have to sign a social contract and adhere to the ethical manifesto. Strict inclusion guidelines make sure that only certified open source software gets packaged in the main repositories.

Fedora is a community edition that serve as the stable basis for enterprise ready GNU/Linux distributions with commercial support. Companies all over the world trust Red Hat Inc. because of their transparency

throughout the whole development process.

Canonical's Ubuntu is not recommended by PRISM Break because it contains Amazon ads and data leaks by default. GNU/Linux distributions based on Ubuntu are also currently not recommended due to several other reasons.

Avoid	✖
Windows	

Operating Systems (Live)

Prefer	✔
Tails Live OS aimed at preserving your privacy and anonymity.	↗
Whonix VM-friendly OS based on Debian and Tor focused on anonymity, privacy and security.	↗

Notes

A live distribution like **Tails** is the fastest and easiest way to a secure operating system. All you have to do is create a bootable CD or USB drive with the files provided and you're set. Everything else will be preconfigured for you.

A virtual machine (VM) image like **Whonix** is designed to be run inside of a virtualization package like VirtualBox. VirtualBox can be installed on Windows, Linux, macOS, and Solaris. This means that if you're stuck using Windows or macOS for whatever reason, you can install VirtualBox and use Whonix to increase your privacy and security.

Password Managers

Prefer	✔
KeePassXC KeePass manager for desktop.	↗

Avoid	✖
1Password	
LastPass	
Roboform	

Productivity

✓

E EtherCalc
Multi-user spreadsheet server.
Web Service ↗

★ Riseup
RiSEUP Secure communication tools for people working on liberatory social change.
Web Service ↗

Notes

Riseup also offers email, XMPP, chat and data hosting (via Up1) services, all of which are accessible through Tor Hidden Service addresses. The list of these addresses is available here.

Avoid ✕

d Doodle

Evernote

Google Docs

GroupWise

Microsoft Outlook

Zoho Docs

Social Networks

Prefer ✓

✱ diaspora*
Community-run, distributed social network.
Web Service ↗

Hubzilla
Platform for creating interconnected websites.
Web Service ↗

Mastodon
Federated microblogging social network.
Web Service ↗

Movim
Private, decentralized social network server.
Web Service ↗

RetroShare

Peer-to-peer communication and file sharing app.

Notes

If you have system administration knowledge, please strongly consider running an instance of **pump.io** (or something else) for your friends, family, or favorite community. Many of them would be willing and grateful to escape Facebook if you provide them a way out.

For those of you without your own server, **RetroShare** is the easiest way to start your own encrypted social network.

Avoid

Facebook

LinkedIn

Snapchat

Twitter

Video & Voice

Prefer

Jami
Decentralized audio/video call app.
Experimental

Mumble
Low-latency multi-user voice chat.

Signal
Metadata-resistant, user-friendly messenger with audio/video calls (mobile only).

Avoid

Discord

Facebook

Skype

TeamSpeak

Ventrilo

VPN

Prefer ✓

Mullvad
No-log WireGuard VPN provider.
Web Service ↗

Riseup
Secure communication tools for people working on liberatory social change.
Web Service ↗

Avoid ✗

Cisco VPN

Hola!

Web Browser Addons

Prefer ✓

Decentraleyes
Protects you against tracking through "free", centralized, content delivery. It prevents a lot of reques… ↗

HTTPS Everywhere
Encrypts your communications from thousands of websites by enforcing HTTPS everywhere. ↗

Mailvelope
OpenPGP browser add-on for webmail. ↗

Multi-Account Containers
Manual identity isolation for Firefox. ↗

NoScript
Only enable JavaScript, Java, and Flash for sites you trust. ↗

Privacy Badger
Tracking blocker that tries to learn who is spying on you and then blocks these ads and invisible tra… ↗

Temporary Containers
Per-tab identity isolation for Firefox.

uBlock Origin
An efficient blocker for Firefox and Chromium. Fast and lean.

Notes

Installing your own add-ons into Tor Browser is not recommended, as they may bypass Tor or otherwise harm your anonymity and privacy. Check the EFF's Panopticlick to see how trackable your browser configuration is by third parties.

If you're using a Firefox-based browser, you can safeguard your browsing habits and stop advertising companies from tracking you by installing **uBlock Origin**, **Request Policy**, and **HTTPS Everywhere**.

A more advanced alternative to **Request Policy** would be **uMatrix**.

Install **NoScript** and enable 'Forbid scripts globally' to improve the security of your browser by preventing 0day JavaScript attacks. This is a drastic option as it will render many websites unusable as they rely heavily on JavaScript. NoScript offers a whitelist you can use to selectively enable JavaScript for sites you trust, but this is considered especially bad for your anonymity if you're using NoScript with **Tor Browser**.

Why is Adblock Plus not recommended? Adblock Plus shows "acceptable ads" by default, which works against the purpose of the add-on. Either disable acceptable ads or use **uBlock Origin** instead.

Avoid

Ghostery

Web Browsers

Prefer

Firefox
Fast, flexible and secure web browser with a vibrant add-on ecosystem.

Tor Browser
Encrypted, anonymous web browsing powered by the Tor network.

Notes

Try to use **Tor Browser** for all of your web surfing. It will offer you far better anonymity than any other browser. Make sure to learn the basics of Tor before using it. If the site you want to visit will not work in Tor Browser, try Firefox intead, but realize these browsers do not anonymize your ip by default.

Tor Browser notes: Using Tor Browser to sign into websites that contain your real ID is counterproductive, and may trip the site's fraud protection. Make sure to check for HTTPS before signing in to a website through Tor. Signing into HTTP websites can result in your ID being captured by a Tor exit node.

Firefox notes: This browser uses Google search by default: replace it with a more private alternative.

Why are Chromium, SRWare Iron, et al. not recommended on PRISM Break? More info here.

Warning for mobile devices & Tor: Websites using HTML5 <video> tags will leak <video>-related DNS queries and data transfer outside of Tor.

Google Chrome

Microsoft Edge

Opera

Yandex.Browser

Web Search

Prefer	✔

DuckDuckGo
Independent no-tracking search engine.
Non-free   Web Service   ↗

Searx
Metasearch engine.
Web Service   ↗

Notes

DuckDuckGo is a software-as-a-service (SaaS) hosted around the world that provides you with anonymous search results from these sources. DDG open source components are available here.

There is also a **DuckDuckGo** hidden service at 3g2upl4pq6kufc4m.onion for Tor users.

MetaGer is a SaaS by the German non-profit SUMA e.V. that provides you with anonymous meta search results.

Startpage is a SaaS hosted in the USA and the Netherlands that provides you with anonymous Google search and image results through a free proxy.

Google Search

Microsoft Bing

Yahoo Search

Yandex

World Maps

Prefer	✔

OpenStreetMap
Free, collaborative world wide map.

Notes

"If you spend time contributing to OpenStreetMap you are helping a good cause, and building a geographic database of the world which is free and open for all and forever."

— OpenStreetMap Wiki

Avoid ✖

Bing Maps

Google Earth

Google Maps

العربية	Català	Deutsch	ελληνικά
Esperanto	English	Español	فارسی
Suomi	Français	עברית	हिन्दी
Ido	Italiano	日本語	Nederlands
Norsk	Polski	Português	Русский
srpski	српски	Svenska	Türkçe
简体中文	繁體中文		