



(<https://www.privacytools.io/>)

You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. privacytools.io provides knowledge and tools to protect your privacy against global mass surveillance.

Privacy? I don't have anything to hide.

(http://www.ted.com/talks/glenn_greenwald_why_privacy_matters) Over the last 16 months, as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." **Not a single person has taken me up on that offer.**

— Glenn Greenwald in *Why privacy matters* - TED Talk (http://www.ted.com/talks/glenn_greenwald_why_privacy_matters)



Related: How do you counter the "I have nothing to hide?" argument? (https://www.reddit.com/r/privacy/comments/3hynvp/how_do_you_counter_the_i_have_nothing_to_hide/)

Privacy-Respecting Search Engine



example search: edward snowden (<https://www.privatesearch.io/?q=Edward%20Snowden>)

privatesearch.io (<https://www.privatesearch.io/>) is our new privacy-respecting and highly customizable search engine with excellent results. It's open source and doesn't have ads, logs or tracking.

🔒 Don't use Windows 10 - It's a privacy nightmare

Microsoft introduced a lot of new features in Windows 10 such as Cortana. However, most of them are violating your privacy.

- 1. Data syncing is by default enabled.**
 - Browsing history and open websites.
 - Apps settings.
 - WiFi hotspot names and passwords.
- 2. Your device is by default tagged with a unique advertising ID.**
 - Used to serve you with personalized advertisements by third-party advertisers and ad networks.
- 3. Cortana can collect any of your data.**
 - Your keystrokes, searches and mic input.
 - Calendar data.
 - Music you listen to.
 - Credit Card information.
 - Purchases.
- 4. Microsoft can collect any personal data.**
 - Your identity.



- Passwords.
- Demographics.
- Interests and habits.
- Usage data.
- Contacts and relationships.
- Location data.
- Content like emails, instant messages, caller list, audio and video recordings.

5. Your data can be shared.

- When downloading Windows 10, you are authorizing Microsoft to share any of above mentioned data with any third-party, with or without your consent.

Source: propakistani.pk (<http://propakistani.pk/2015/07/30/windows-10-can-be-your-worst-privacy-nightmare/>)

Download: Win10 Tracking Disable Tool (<https://github.com/10se1ucgo/DisableWinTracking/releases>)

This open source tool uses some known methods that attempt to disable major tracking features in Windows 10.

More bad news

- Even when told not to, Windows 10 just can't stop talking to Microsoft. It's no wonder that privacy activists are up in arms. (<http://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/>) - Ars Technica.
- Windows 10 privacy paranoia leads to ban from private pirate torrent trackers. Pirates are concerned that Win10 will send the contents of your hard disk to Microsoft. (<http://arstechnica.com/information-technology/2015/08/windows-10-privacy-paranoia-leads-to-ban-from-private-piracy-torrent-trackers/>) - Ars Technica.
- What Windows 10's "Privacy Nightmare" Settings Actually Do. (<http://lifehacker.com/what-windows-10s-privacy-nightmare-settings-actually-1722267229>) - Lifehacker.
- Windows 10 Reserves The Right To Block Pirated Games And 'Unauthorized' Hardware. (<https://www.techdirt.com/articles/20150820/06171332012/windows-10-reserves-right-to-block-pirated-games-unauthorized-hardware.shtml>) - Techdirt.

Some good news

- Fix Windows 10 privacy. (<https://fix10.isleaked.com/>) - fix10.isleaked.com
- Windows 10 doesn't offer much privacy by default: Here's how to fix it. (<http://arstechnica.com/information-technology/2015/08/windows-10-doesnt-offer-much-privacy-by-default-heres-how-to-fix-it/>) - Ars Technica.
- Guide: How to disable data logging in W10. (https://www.reddit.com/r/Windows10/comments/3f38ed/guide_how_to_disable_data_logging_in_w10)

🕵️ Global Mass Surveillance - The Fourteen Eyes

The UKUSA Agreement is an agreement between the United Kingdom, United States, Australia, Canada, and New Zealand to cooperatively collect, analyze, and share intelligence. Members of this group, known as the Five Eyes (<http://www.giswatch.org/en/communications-surveillance/unmasking-five-eyes-global-surveillance-practices>), focus on gathering and analyzing intelligence from different parts of the world. While Five Eyes countries have agreed to not spy on each other (<http://www.pbs.org/newshour/rundown/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other/>) as adversaries, leaks by Snowden have revealed that some Five Eyes members monitor each other's citizens and share intelligence (<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>) to avoid breaking domestic laws (<http://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett>) that prohibit them from spying on their own citizens. The Five Eyes alliance also cooperates with groups of third party countries to share intelligence (forming the Nine Eyes and Fourteen Eyes), however Five Eyes and third party countries can and do spy on each other.



Five Eyes	Nine Eyes	Fourteen Eyes
1. Australia 2. Canada 3. New Zealand 4. United Kingdom 5. United States of America	6. Denmark 7. France 8. Netherlands 9. Norway	10. Belgium 11. Germany 12. Italy 13. Spain 14. Sweden

Why is it not recommended to choose a US based service?

Services based in the United States are not recommended because of the country's surveillance programs, use of National Security Letters (<https://www.eff.org/issues/national-security-letters/faq>) (NSLs) and accompanying gag orders, which forbid the recipient from talking about the request. This combination allows the government to secretly force (https://www.schneier.com/blog/archives/2013/08/more_on_the_nsa.html) companies to grant complete access to customer data and transform the service into a tool of mass surveillance.

An example of this is Lavabit (http://en.wikipedia.org/wiki/Lavabit#Suspension_and_gag_order) - a discontinued secure email service created by Ladar Levison. The FBI requested (<http://motherboard.vice.com/blog/lavabit-founder-ladar-levison-discusses-his-federal-battle-for-privacy>) Snowden's records after finding out that he used the service. Since Lavabit did not keep logs and email content was stored encrypted, the FBI served a subpoena (with a gag order) for the service's SSL keys. Having the SSL keys would allow them to access communications (both metadata and unencrypted content) in real time for all of Lavabit's customers, not just Snowden's.

Ultimately, Levison turned over the SSL keys and shut down (<http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>) the service at the same time. The US government then threatened Levison with arrest (<http://www.cnn.com/id/100962389>), saying that shutting down the service was a violation of the court order.

Key disclosure law - Who is required to hand over the encryption keys to authorities?

Mandatory key disclosure laws require individuals to turn over encryption keys to law enforcement conducting a criminal investigation. How these laws are implemented (who may be legally compelled to assist) vary from nation to nation, but a warrant is generally required. Defenses against key disclosure laws include steganography and encrypting data in a way that provides plausible deniability.

Steganography involves hiding sensitive information (which may be encrypted) inside of ordinary data (for example, encrypting an image file and then hiding it in an audio file). With plausible deniability, data is encrypted in a way that prevents an adversary from being able to prove that the information they are after exists (for example, one password may decrypt benign data and another password, used on the same file, could decrypt sensitive data).







Related Information

- Avoid all US and UK based services (<https://www.bestvpn.com/the-ultimate-privacy-guide/#avoidus>)
- Proof that warrant canaries work based on the surespot example. (<https://en.wikipedia.org/wiki/Surespot#History>)
- http://en.wikipedia.org/wiki/UKUSA_Agreement (http://en.wikipedia.org/wiki/UKUSA_Agreement)
- http://en.wikipedia.org/wiki/Lavabit#Suspension_and_gag_order (http://en.wikipedia.org/wiki/Lavabit#Suspension_and_gag_order)
- https://en.wikipedia.org/wiki/Key_disclosure_law (https://en.wikipedia.org/wiki/Key_disclosure_law)
- http://en.wikipedia.org/wiki/Portal:Mass_surveillance (http://en.wikipedia.org/wiki/Portal:Mass_surveillance)



🔑 VPN providers with extra layers of privacy - No Affiliates





All providers listed here are outside the US, use encryption, accept Bitcoin, support OpenVPN and have a no logging policy. Prices are yearly. The table is sortable.

First Half

VPN / Country	Servers	Price
 AirVPN.org (Italy) (https://airvpn.org/)	76	54 €
 AzireVPN.com (Sweden) (https://www.azirevpn.com/)	3	45 €
 blackVPN.com (Hong Kong) (https://www.blackvpn.com/)	25	99 €
 Cryptostorm.is (Iceland) (https://cryptostorm.is/)	13	\$ 52
 FrootVPN.com (Sweden) (https://www.frootvpn.com/)	27	\$ 36
 hide.me (Malaysia) (https://hide.me/)	85	\$ 65

Second Half

VPN / Country	Servers	Price
 IVPN.net (Gibraltar) (https://www.ipvn.net/)	15	\$ 100
 Mullvad.net (Sweden) (https://mullvad.net/)	23	60 €

VPN / Country	Servers	Price
 NordVPN.com (Panama) (https://nordvpn.com/)	52	\$ 48
 Perfect-Privacy.com (Panama) (https://www.perfect-privacy.com/)	40	150 €
 Privatoria.net (Czech Republic) (https://privatoria.net/)	12	\$ 22,8
 Proxy.sh (Seychelles) (https://proxy.sh/)	288	\$ 90

Note: Using a VPN provider will not make you anonymous. But it will give you a better privacy. A VPN is not a tool for illegal activities. Don't rely on a "no log" policy.

Our VPN Provider Criteria

- Operating outside the USA or other Five Eyes countries. Avoid all US and UK based services. (<https://www.bestvpn.com/the-ultimate-privacy-guide/#avoidus>)
- OpenVPN software support.
- File-Sharing (P2P) is tolerated on selected servers.
- Accepts Bitcoin, cash, debit cards or cash cards as a payment method.
- No personal information is required to create an account. Only username, password and Email.

We're not affiliated with any of the above listed VPN providers. This way can give you honest recommendations.

Related VPN information

- How To Make VPNs Even More Secure (<http://torrentfreak.com/how-to-make-vpns-even-more-secure-120419/>)
- VPN, privacy and anonymity - SpiderOak (<https://blog.spideroak.com/20140124105217-vpn-privacy-anonymity>)
- Beware of False Reviews - VPN Marketing and Affiliate Programs (<https://vikingvpn.com/blogs/off-topic/beware-of-vpn-marketing-and-affiliate-programs>)
- Which VPN Services Take Your Anonymity Seriously? (<http://torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/>)
(**Note:** The providers listed first in the TorrentFreaks article are sponsored)
- I am Anonymous When I Use a VPN - 7 Myths Debunked (<https://www.goldenfrog.com/take-back-your-internet/articles/7-myths-about-vpn-logging-and-anonymity>)
(**Note:** While this is a good read, they also use the article for self promotion)
- Proxy.sh VPN Provider Sniffed Server Traffic to Catch Hacker (<http://torrentfreak.com/proxy-sh-vpn-provider-monitored-traffic-to-catch-hacker-130930/>)
- Ethical policy - All of the reasons why Proxy.sh might enable logging (<https://proxy.sh/panel/knowledgebase.php?action=displayarticle&id=5>)
- IVPN.net will collect your email and IP address after sign up (<https://www.ipvn.net/privacy>)
Read the Email statement from IVPN.
- blackVPN announced to delete connection logs after disconnection (<https://medium.com/@blackVPN/no-logs-6d65d95a3016>)

What is a warrant canary?

A warrant canary is a posted document stating that an organization has not received any secret subpoenas during a specific period of time. If this document fails to be updated during the specified time then the user is to assume that the service has received such a subpoena and should stop using the service.

Warrant Canary Examples:

1. <https://proxy.sh/canary> (<https://proxy.sh/canary>)
2. <https://www.ipvn.net/resources/canary.txt> (<https://www.ipvn.net/resources/canary.txt>)
3. <https://www.vpnsecure.me/files/canary.txt> (<https://www.vpnsecure.me/files/canary.txt>)
4. <https://www.bolehvpn.net/canary.html> (<https://www.bolehvpn.net/canary.html>)
5. <https://lokun.is/canary.txt> (<https://lokun.is/canary.txt>)
6. <https://www.ipredator.se/static/downloads/canary.txt> (<https://www.ipredator.se/static/downloads/canary.txt>)


Related Warrant Canary Information

- Warrant Canary Frequently Asked Questions (<https://www.eff.org/de/deepinks/2014/04/warrant-canary-faq>)
- Canarywatch.org (<https://canarywatch.org/>) - Lists warrant canaries, tracks changes or disappearances of canaries
- Companies and organizations with warrant canaries (http://en.wikipedia.org/wiki/Warrant_canary#Companies_and_organizations_with_warrant_canaries)

**The FBI
has not
been here**

(watch very closely for the removal of this sign)

🔗 Browser Recommendation



Firefox

(<http://www.erfahrungen.com/mit/Firefox/>) is fast, reliable, open source and respects your privacy. Don't forget to adjust the settings according to our recommendations: WebRTC and about:config and get the privacy addons.

Download: www.firefox.com
(<https://www.firefox.com/>)

OS: Windows, Mac, Linux, Android, BSD.

Tor Browser Bundle

Tor Browser is your choice if you need an extra layer of anonymity. It's a modified version of Firefox, it comes with pre-installed privacy addons, encryption and an advanced proxy.

Download: www.torproject.org
(<https://www.torproject.org/>)

OS: Windows, Mac, Linux, iOS
(<https://mike.tig.as/onionbrowser/>), Android
(<https://www.torproject.org/docs/android.html.en>), OpenBSD.
(<https://github.com/torbsd/openbsd-ports>)

Worth Mentioning

- JonDoFox (<https://anonymous-proxy-servers.net/en/jondofox.html>) - A profile for the Firefox web browser, particularly optimized for anonymous and secure web surfing.

🔗 Browser Fingerprint - Is your browser configuration unique?

Your Browser sends information that makes you unique amongst millions of users and therefore easy to identify.

When you visit a web page, your browser voluntarily sends information about its configuration, such as available fonts, browser type, and add-ons. If this combination of information is unique, it may be possible to identify and track you without using cookies. EFF created a Tool called Panoptlick (<https://panoptlick.eff.org/>) to test your browser to see how unique it is.

Test your Browser now

(<https://panoptlick.eff.org/>)

You need to find what **most browsers** are reporting, and then use those variables to bring your browser in the same population. This means having the same fonts, plugins, and extensions installed as the large installed base. You should have a spoofed user agent string (<https://addons.mozilla.org/en-US/firefox/addon/random-agent-spoof/>) to match what the large userbase has. You need have the same settings enabled and disabled, such as DNT and WebGL. You need your browser to look as common as everyone else. Disabling JavaScript, using Linux, or even the TBB, will make your browser stick out from the masses.

Modern web browsers have not been architected to assure personal web privacy. Rather than worrying about being fingerprinted, it seems more practical to use free software plugins like Privacy Badger, uBlock Origin and Disconnect. They not only respect your freedom, but your privacy also. You can get much further with these than trying to manipulate your browser's fingerprint.

Related Information

- How Unique Is Your Web Browser? Peter Eckersley, EFF. (<https://panoptlick.eff.org/browser-uniqueness.pdf>)
- Join our discussion on reddit.com about browser fingerprinting. (https://www.reddit.com/r/privacytoolsio/comments/35pqyl/new_section_browser_fingerprint_is_your_browser/)
- Our Firefox privacy addons section.
- BrowserLeaks.com (<https://www.browserleaks.com/>) - Web browser security testing tools, that tell you what exactly personal identity data may be leaked without any permissions when you surf the Internet.

🔗 WebRTC IP Leak Test - Is your IP address leaking?

WebRTC is a new communication protocol that relies on JavaScript that can leak your actual IP address from behind your VPN.

While software like NoScript prevents this, it's probably a good idea to block this protocol directly as well, just to be safe.

[Test your Browser now](#) (webrtc.html)

How to disable WebRTC in Firefox?

In short: Set "media.peerconnection.enabled" to "false" in "about:config".

Explained:

1. Enter "about:config" in the Firefox address bar and press enter.
2. Press the button "I'll be careful, I promise!"
3. Search for "media.peerconnection.enabled"
4. Double click the entry, the column "Value" should now be "false"
5. Done. Do the WebRTC leak test again.

If you want to make sure every single WebRTC related setting is really disabled change these settings:

1. media.peerconnection.turn.disable = true
2. media.peerconnection.use_document_iceservers = false
3. media.peerconnection.video.enabled = false
4. media.peerconnection.identity.timeout = 1

Now you can be 100% sure WebRTC is disabled.

[Test your Browser again](#) (webrtc.html)

How to fix the WebRTC Leak in Google Chrome?

There is no known working solution, only a plugin that is easily circumvented. Please use Firefox instead.

What about other browsers?

Chrome on iOS, Internet Explorer and Safari does not implement WebRTC yet. But we recommend using Firefox on all devices.

Excellent Firefox Privacy Addons

Improve your privacy with these excellent Firefox addons.

Stop tracking with "Disconnect"



Disconnect was founded in 2011 by former Google engineers and a consumer-and privacy-rights attorney. The addon is open source and loads the pages you go to 27% faster and stops tracking by 2,000+ third-party sites. It also keeps your searches

private.

<https://addons.mozilla.org/en-US/firefox/addon/disconnect/> (<https://addons.mozilla.org/en-US/firefox/addon/disconnect/>)

Block Ads with "uBlock Origin"



uBlock Origin is a lightweight and efficient blocker: easy on memory and CPU footprint. The extension has no monetization strategy and development is volunteered. OS: Firefox, Safari, Opera, Chromium. Adblock Plus is not recommended because

they show "acceptable ads". The system behind that white list is lacking transparency.

<https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/> (<https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>)

Hinder Browser Fingerprinting with "Random Agent Spoofer"



Random Agent Spoofer is a privacy enhancing Firefox addon which aims to hinder browser fingerprinting. It does this by changing the browser/device profile on a timer.

<https://addons.mozilla.org/en-US/firefox/addon/random-agent-spoofers/>

(<https://addons.mozilla.org/en-US/firefox/addon/random-agent-spoofers/>)

Automatically Delete Cookies with "Self-Destructing Cookies"



Self-Destructing Cookies automatically removes cookies when they are no longer used by open browser tabs. With the cookies, lingering sessions, as well as information used to spy on you, will be expunged.

<https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/> (<https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/>)

Encryption with "HTTPS Everywhere"



HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. A collaboration between The Tor Project and the Electronic Frontier Foundation.

<https://www.eff.org/https-everywhere> (<https://www.eff.org/https-everywhere>)

The following addons require quite a lot of interaction from user to get things working. Some sites will not work properly until you have configured the addons.

Be in total control with "NoScript Security Suite"




Highly customizable plugin to selectively allow Javascript, Java, and Flash to run only on websites you trust. Not for casual users, it requires technical knowledge to configure.

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

(<https://addons.mozilla.org/en-US/firefox/addon/noscript/>)

Content control with "Policeman"



This add-on has purpose similar to RequestPolicy and NoScript. It's different from the former in that it supports rules based on content type. For example, you can allow images and styles, but not scripts and frames for some sites. It can also be set up to act as a blacklist.

<https://addons.mozilla.org/en-US/firefox/addon/policeman/> (<https://addons.mozilla.org/en-US/firefox/addon/policeman/>)

Firefox: Privacy Related "about:config" Tweaks


This is a collection of privacy related **about:config** tweaks. We'll show you how to enhance the privacy of your Firefox browser.













- Preparation:
1. Enter "about:config" in the firefox address bar and press enter.
 2. Press the button "I'll be careful, I promise!"
 3. Follow the instructions below...
- Getting started:
1. `privacy.trackingprotection.enabled = true`
 - This is Mozilla's new built in tracking protection.
 2. `geo.enabled = false`
 - Disables geolocation.
 3. `browser.safebrowsing.enabled = false`
 - Disable Google Safe Browsing and phishing protection. Security risk, but privacy improvement.
 4. `browser.safebrowsing.malware.enabled = false`
 - Disable Google Safe Browsing malware checks. Security risk, but privacy improvement.
 5. `dom.event.clipboardevents.enabled = false`
 - Disable that websites can get notifications if you copy, paste, or cut something from a web page, and it lets them know which part of the page had been selected.
 6. `network.cookie.cookieBehavior = 1`
 - Disable cookies
 - 0 = accept all cookies by default
 - 1 = only accept from the originating site (block third party cookies)
 - 2 = block all cookies by default
 7. `network.cookie.lifetimePolicy = 2`
 - cookies are deleted at the end of the session
 - 0 = Accept cookies normally
 - 1 = Prompt for each cookie
 - 2 = Accept for current session only
 - 3 = Accept for N days
 8. `browser.cache.offline.enable = false`
 - Disables offline cache.
 9. `browser.send_pings = false`
 - The attribute would be useful for letting websites track visitors' clicks.
 10. `webgl.disabled = true`
 - WebGL is a potential security risk. Source (<http://security.stackexchange.com/questions/13799/is-webgl-a-security-concern>)
 11. `dom.battery.enabled = false`
 - Website owners can track the battery status of your device. Source (https://www.reddit.com/r/privacytoolsIO/comments/3fzbgg/you_may_be_tracked_by_your_battery_status_of_your/)
 12. `browser.sessionstore.max_tabs_undo = 0`
 - Even with Firefox set to not remember history, your closed tabs are stored temporarily at Menu -> History -> Recently Closed Tabs.

- Related Information
- [mozillazine.org](http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences) (http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences) - Security and privacy-related preferences.
 - [user.js](https://github.com/pyllyukko/user.js) Firefox hardening stuff (<https://github.com/pyllyukko/user.js>) - This is a user.js configuration file for Mozilla Firefox that's supposed to harden Firefox's settings and make it more secure.

Privacy-Conscious Email Providers - No Affiliates

All providers listed here are operating outside the US and support SMTP TLS. The table is sortable. Never trust any company with your privacy, always encrypt.

Email Service	Since	Server	Storage	Price / Year	Bitcoin	Encryption	Own Domain
 GhostMail.com (https://www.ghostmail.com/)	2015	Sweden	1 GB	Free	Accepted	Built-in	No

Email Service	Since	Server	Storage	Price / Year	Bitcoin	Encryption	Own Domain
 OpenMailBox.org (https://www.openmailbox.org/)	2013	France	1 GB	Free	Accepted	Built-in	No
 ProtonMail.ch (https://www.protonmail.ch/)	2013	Switzerland	500 MB	Free	Accepted	Built-in	No
 Tutanota.com (https://www.tutanota.com/)	2011	Germany	1 GB	Free	Accepted	Built-in	Yes
 whiteout.io (https://whiteout.io/)	2014	Germany	2 GB	Free	No	Built-in	No
 mailbox.org (https://www.mailbox.org/)	2014	Germany	2 GB	12 €	Accepted	Built-in	Yes
 Posteo.de (https://www.posteo.de/)	2009	Germany	2 GB	12 €	No	Built-in	No
 Runbox.com (https://runbox.com/)	1999	Norway	1 GB	\$ 19.95	No	No	Yes
 Neomailbox.com (https://www.neomailbox.com/)	2003	Switzerland	1 GB	\$ 49.95	Accepted	Built-in	Yes
 CounterMail.com (https://www.countermail.com/)	2010	Sweden	500 MB	\$ 59	Accepted	Built-in	Yes
 StartMail.com (https://www.startmail.com/)	2014	Netherlands	10 GB	\$ 59.95	No	Built-in	No
 KolabNow.com (https://www.kolabnow.com/)	2010	Switzerland	2 GB	\$ 60	Accepted	No	Yes
 CryptoHeaven.com (http://www.cryptoheaven.com/)	2001	Canada	200 MB	\$ 66	No	Built-in	Yes

Interesting Email Providers Under Development

- Confidant Mail (<https://www.confidantmail.org/>) - An open-source non-SMTP cryptographic email system optimized for large file attachments. It is a secure and spam-resistant alternative to regular email and online file drop services. It uses GNU Privacy Guard (GPG) for content encryption and authentication, and TLS 1.2 with ephemeral keys for transport encryption.

Become Your Own Email Provider with Mail-in-a-Box

 Mail-in-a-Box
 (https://mailinabox.email/)

Take it a step further and get control of your email with this easy-to-deploy mail server in a box. Mail-in-a-Box lets you become your own mail service provider in a few easy steps. It's sort of like making your own gmail, but one you control from top to bottom. Technically, Mail-in-a-Box turns a fresh cloud computer into a working mail server. But you don't need to be a technology expert to set it up. **More:** <https://mailinabox.email/> (<https://mailinabox.email/>)

Privacy Email Tools

- **gpg4usb** (<http://www.gpg4usb.org/>) - A very easy to use and small portable editor to encrypt and decrypt any text-message or -file. For Windows and Linux.
- **Mailvelope** (<https://www.mailvelope.com/>) - A browser extension that enables the exchange of encrypted emails following the OpenPGP encryption standard.
- **Enigmail** (<https://www.enigmail.net/>) - A security extension to Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.
- **TorBirdy** (<https://addons.mozilla.org/en-us/thunderbird/addon/torbirdy/>) - This extension configures Thunderbird to make connections over the Tor anonymity network.
- **Email Privacy Tester** (<https://emailprivacytester.com/>) - This tool will sent an Email to your address and perform privacy related tests.


Related Information

- **Aging 'Privacy' Law Leaves Cloud E-Mail Open to Cops** (<http://www.wired.com/2011/10/ecpa-turns-twenty-five/>) - Data stored in the cloud for longer than 6 months is considered abandoned and may be accessed by intelligence agencies without a warrant. Learning: Use an external email client like Thunderbird or Enigmail, download your emails and store them locally. Never leave them on the server.
- **OpenMailBox keeps one year logs of meta-data** (<https://www.openmailbox.org/forum/viewtopic.php?id=390>) - Forum discussion, reply of the server admin.
- **With May First/Riseup Server Seizure, FBI Overreaches Yet Again** (<https://www.eff.org/deeplinks/2012/04/may-first-riseup-server-seizure-fbi-overreaches-yet-again>)
- **Autistici/Inventati server compromised** (<http://www.autistici.org/ai/crackdown/>) - The cryptographic services offered by the Autistici/Inventati server have been compromised on 15th June 2004. It was discovered on 21st June 2005. One year later. During an enquiry on a single mailbox, the Postal Police may have tapped for a whole year every user's private communication going through the server [autistici.org/inventati.org](http://www.autistici.org/inventati.org).

Email Clients

Thunderbird

Mozilla




Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation. Thunderbird is an email, newsgroup, news feed, and chat (XMPP, IRC, Twitter) client.

Website: [mozilla.org](https://mozilla.org/thunderbird)
(<https://mozilla.org/thunderbird>)

OS: Windows, Mac, Linux, BSD.

Claws Mail

Claws Mail is a free and open source,




GTK+-based email and news client. It offers easy configuration and an abundance of features. It is included with Gpg4win, an encryption suite for Windows.

Website: [claws-mail.org](http://www.claws-mail.org)
(<http://www.claws-mail.org/>)

OS: Windows, Mac, Linux, BSD, Solaris, Unix.

Whiteout Mail



Whiteout Mail is an open source email solution with strong end-to-end encryption that is really easy to use and runs on all of your devices. Keeping your emails safe has never been so easy. You can also get a new email address.

Website: whiteout.io
(<https://whiteout.io/>)


OS: Chrome, Android, iOS, Web.

Worth Mentioning

- **K-9 Mail** (<https://github.com/k9mail/k-9/releases>) - An independent mail application for Android. It supports both POP3 and IMAP mailboxes, but only supports push mail for IMAP.
- **GNU Privacy Guard** (<https://www.gnupg.org/>) - Email Encryption. GnuPG is a GPL Licensed alternative to the PGP suite of cryptographic software. Use GPGTools for Mac OS X. (<https://gpgtools.org/>)
- **Mailpile (Beta)** (<https://www.mailpile.is/>) - A modern, fast web-mail client with user-friendly encryption and privacy features.

Email Alternatives


Bitmessage



Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities. It uses strong authentication which means that the sender of a message cannot be spoofed, and it aims to hide

I2P-Bote

I2P-Bote is a fully




decentralized and distributed email system. It supports different identities and does not expose email headers. Currently (2015), it is still in beta version and can be accessed via its web application interface or IMAP and SMTP. All bote-mails are transparently end-to-end encrypted and, optionally, signed by the sender's private key.

Website: i2pbote.i2p.us

Pond - Experimental

Pond is forward secure,



asynchronous messaging for the discerning. Pond messages are asynchronous, but are not a record; they expire automatically a week after they are received. Pond seeks to prevent leaking traffic information against everyone except a global passive attacker. Build instructions are OS: Ubuntu, Debian Wheezy, Tails, Fedora, Arch and Mac OS X.

"non-content" data.

Website: bitmessage.org
(<https://bitmessage.org/>)

OS: Windows, Mac,
Linux.

(<http://i2pbote.i2p.us/>)

OS: Windows, Mac,
Linux, Android, F-Droid.

Website: pond.imperialviolet.org
(<https://pond.imperialviolet.org/>)

OS: Mac, Linux.

Worth Mentioning


- RetroShare (<http://retroshare.sourceforge.net/>) - Open Source cross-platform, Friend-2-Friend and secure decentralised communication platform.

Privacy Respecting Search Engines

If you are currently using a search engines like Google, Bing or Yahoo you should pick an alternative here.

privatesearch.io

An open source




(<https://github.com/asciimoo/searx>) metasearch engine, aggregating the results of other search engines while not storing information about its users. No logs, no ads and no tracking.

Website: [privatesearch.io](https://www.privatesearch.io/)
(<https://www.privatesearch.io/>)

DuckDuckGo

The search engine that doesn't track you. Some of DuckDuckGo's code is free software hosted at GitHub (<https://github.com/duckduckgo>), but the core is proprietary. The company is based in the USA.




Website: duckduckgo.com
(<https://duckduckgo.com/>)

Tor Link
(<http://3g2upl4pq6kufc4m.onion/>)

Disconnect Search

Search



privately using your favorite search engine: Google, Yahoo, Bing and DuckDuckGo are available for selection. It masks your IP address, cookies, and other personal info.

Website: search.disconnect.me
(<https://search.disconnect.me/>)


Worth Mentioning

- MetaGer (<https://metager.de/en/>) - A metasearch engine, which is based in Germany. It focuses on protecting the user's privacy. Supported by 24 own crawlers of small scale web search engines.
- ixquick.com (<https://ixquick.com/>) - Returns the top ten results from multiple search engines. It uses a "Star System" to rank its results by awarding one star for every result that has been returned from a search engine. Based in the USA and the Netherlands.
- Google search link fix (<https://addons.mozilla.org/en-us/firefox/addon/google-search-link-fix/>) - Firefox extension that prevents Google, Yahoo and Yandex search pages from modifying search result links when you click them. This is useful when copying links but it also helps privacy by preventing the search engines from recording your clicks. (Open Source (<https://github.com/palant/searchlinkfix>))

Encrypted Instant Messenger

If you are currently using an Instant Messenger like WhatsApp, Viber, LINE or Threema you should pick an alternative here.


Most Secure: ChatSecure



ChatSecure is a free and open source messaging app that features OTR encryption over XMPP. You can connect to your existing accounts on Facebook or Google, create new accounts on public XMPP servers (including via Tor), or even connect to your own server for extra security. ChatSecure only uses well-known open source cryptographic libraries to keep your conversations private.


Download: www.chatsecure.org

Mobile: TextSecure / Signal



TextSecure and Signal are mobile apps developed by Open Whisper Systems. The company also developed RedPhone (<https://whispersystems.org/>). All three apps are able to communicate with each other. The apps provide end-to-end encryption for your text messages. TextSecure is free and open source, enabling anyone to verify its security by auditing the code. Encrypted group chats are also supported.

Good for Browsers: Cryptocat




Cryptocat is an open source web and mobile application intended to allow secure, encrypted online chatting. Cryptocat uses end-to-end encryption and encrypts chats on the client side, only trusting the server with data that is already encrypted. Cryptocat's stated goal is to make encrypted communications more accessible to average users.

Download: www.cryptocat.net



Seafile offers 100 GB Storage for




\$10/month but also gives you the opportunity to host on your own server. Your data is stored in Germany or with Amazon Web Service in the US for the cloud version. Encrypt files with your own password.

Website: seafile.com
(<http://seafile.com/>)

Client OS: Windows, Mac, Linux, iOS, Android.
Server: Linux, Raspberry Pi, Windows.

Similar



functionally to the widely used Dropbox, with the difference being that ownCloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

Website: owncloud.org
(<https://owncloud.org/providers/>)

Client OS: Windows, Mac, Linux, BSD, Unix, iOS, Android, Fire OS. Server: Linux.

S4 (Simple Secure Storage Service) is Least Authority's verifiably secure off-site backup system for individuals and businesses. 100% client-side encryption and open source transparency. \$25/month for unlimited storage. Servers are hosted with Amazon S3 in the US.

Website: leastaauthority.com
(<https://leastaauthority.com/>)

OS: Linux (<https://tahoe-lafs.org/trac/tahoe-lafs/wiki/Installation>), Windows, Mac, OpenSolaris, BSD. (<https://tahoe-lafs.org/trac/tahoe-lafs/browser/trunk/docs/quickstart.rst>) (Installation for advanced users)

Related Information


- Cryptomator (<https://cryptomator.org/>) - Free client-side AES encryption for your cloud files. Open source software: No backdoors, no registration. Beta software.
- reddit.com (https://www.reddit.com/r/privacytoolsio/comments/31v6ma/should_spideroak_be_avoided/) - Should SpiderOak be avoided? Read the discussion in our subreddit.

Self-Hosted Cloud Server Software

If you are currently using a Cloud Storage Services like Dropbox, Google Drive, Microsoft OneDrive or Apple iCloud you should think about hosting it on your own.

Seafile

Seafile is a file hosting




software system. Files are stored on a central server and can be synchronized with personal computers and mobile devices via the Seafile client. Files can also be accessed via the server's web interface.

Website: seafile.com
(<http://seafile.com/>)

Client OS: Windows, Mac, Linux, iOS, Android.
Server: Linux, Raspberry Pi, Windows.

Pydio

Pydio is open source




software that turns instantly any server (on premise, NAS, cloud IaaS or PaaS) into a file sharing platform for your company. It is an alternative to SaaS Boxes and Drives, with more control, safety and privacy, and favorable TCOs.

Website: pydio.io
(<https://pydio.io/>)

OS: Windows, Mac, Linux, iOS, Android.

Tahoe-LAFS



Tahoe-LAFS is a Free and Open decentralized cloud storage system. It distributes your data across multiple servers. Even if some of the servers fail or are taken over by an attacker, the entire file store continues to function correctly, preserving your privacy and security.

Website: [tahoe-lafs.org](https://www.tahoe-lafs.org/)
(<https://www.tahoe-lafs.org/>)


OS: Windows, Mac, Linux.

Worth Mentioning

- ownCloud (<https://owncloud.org/>) - Free and open-source, allows anyone to install and operate it for free on a private server, with no limits on storage space or the number of connected clients.


Secure File Sync Software

SparkleShare




Syncany

Syncany allows users to backup and share



Syncthing



SparkleShare creates a special folder on your computer. You can add remotely hosted folders (or "projects") to this folder. These projects will be automatically kept in sync with both the host and all of your peers when someone adds, removes or edits a file.

Website: sparkleshare.org
(<http://sparkleshare.org/>)

OS: Windows, Mac, Linux.

certain folders of their workstations using any kind of storage. Syncany is open-source and provides data encryption and incredible flexibility in terms of storage type and provider. Files are encrypted before uploading.

Website: [syncany.org](https://www.syncany.org)
(<https://www.syncany.org/>)

OS: Windows, Mac, Linux.

Syncething replaces proprietary sync and cloud services with something open, trustworthy and decentralized. Your data is your data alone and you deserve to choose where it is stored, if it is shared with some third party and how it's transmitted over the Internet.

Website: syncething.net
(<https://syncething.net/>)

OS: Windows, Mac, Linux, Android, BSD, Solaris.

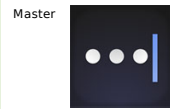
Worth Mentioning

- git-annex (<https://git-annex.branchable.com/>) - Allows managing files with git, without checking the file contents into git. While that may seem paradoxical, it is useful when dealing with files larger than git can currently easily handle, whether due to limitations in memory, time, or disk space..

🔗 Password Manager Software

If you are currently using a password manager software like 1Password, LastPass, Roboform or iCloud Keychain you should pick an alternative here.

Master Password - Cross-platform



Password is based on an ingenious password generation algorithm that guarantees your passwords can never be lost. Its passwords aren't stored: they are generated on-demand from your name, the site and your master password. No syncing, backups or internet access needed.

Website: [masterpasswordapp.com](https://ssl.masterpasswordapp.com/)
(<https://ssl.masterpasswordapp.com/>)

OS: Windows, Mac, Linux, iOS, Android, Web.

KeePass / KeePassX - Local



password manager, which helps you to manage your passwords in a secure way. All passwords in one database, which is locked with one master key or a key file. The databases are encrypted using the best and most secure encryption algorithms currently known: AES and Twofish. See also: KeePassX

Website: www.keeppassx.org
(<http://www.keeppassx.org/>)

Website: [keepass.info](http://keepass.info/download.html)
(<http://keepass.info/download.html>)
OS: Windows, Mac, Linux, iOS, Android, BSD.

Encryptr - Cloud Based



Encryptr is simple and easy to use. It stores your sensitive data like passwords, credit card data, PINs, or access codes, in the cloud. However, because it was built on the zero knowledge Crypton framework, Encryptr ensures that only the user has the ability to access or read the confidential information.

Website: encryptr.org
(<https://encryptr.org/>)

OS: Windows, Mac, Linux, Android.

Worth Mentioning

- Secure Password Generator (<https://www.privacytools.io/password.html%09>) - generates a unique set of custom, high quality, cryptographic-strength password strings which are safe for you to use.
- SuperGenPass (<http://www.supergenpass.com/>) - A master password and the domain name of the Web site you are visiting is used as the "seed" for a one-way hash algorithm (base-64 MD5). The output of this algorithm is your generated password. You remember one password (your "master password"), and SGP uses it to generate unique, complex passwords for the Web sites you visit. Your generated passwords are never stored or transmitted, so you can use SGP on as many computers as you like without having to "sync" anything.
- Password Safe (<http://pwsafe.org/>) - Whether the answer is one or hundreds, Password Safe allows you to safely and easily create a secured and encrypted user name/password list. With Password Safe all you have to do is create and remember a single "Master Password" of your choice in order to unlock and access your entire user name/password list.

Related Information

- Edward Snowden on Passwords - YouTube (<https://www.youtube.com/watch?v=yZgZB-yYKcc>)

🔗 File Encryption Software

If you are currently not using encryption software for your hard disk, emails or file

archives you should pick an encryption software here.

VeraCrypt - Disk Encryption



VeraCrypt is a source-available freeware utility used for on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication. VeraCrypt is a fork of the discontinued TrueCrypt project. It was initially released on June 22, 2013. According to its developers, security improvements have been implemented and issues raised by the initial TrueCrypt code audit have been addressed.

Website: veracrypt.codeplex.com
(<https://veracrypt.codeplex.com/>)

OS: Windows, Mac, Linux.

GNU Privacy Guard - Email Encryption

GnuPG is a GPL



Licensed alternative to the PGP suite of cryptographic software. GnuPG is compliant with RFC 4880, which is the current IETF standards track specification of OpenPGP. Current versions of PGP (and Veridis' Filecrypt) are interoperable with GnuPG and other OpenPGP-compliant systems. GnuPG is a part of the Free Software Foundation's GNU software project, and has received major funding from the German government. GPGTools for Mac OS X.

Website: gnupg.org
(<https://www.gnupg.org/>)

OS: Windows, Mac, Linux, Android, BSD.

PeaZip - File Archive Encryption

PeaZip is a free and



open-source file manager and file archiver made by Giorgio Tani. It supports its native PEA archive format (featuring compression, multi volume split and flexible authenticated encryption and integrity check schemes) and other mainstream formats, with special focus on handling open formats. It supports 181 file extensions (as of version 5.5.1).

Mac alternative: Keka (<http://www.kekaosx.com/>) is a free file archiver.

Website: [peazip.org](http://www.peazip.org)
(<http://www.peazip.org/>)

OS: Windows, Linux, BSD.

Worth Mentioning

- Cryptomator (<https://cryptomator.org/>) - Free client-side AES encryption for your cloud files. Open source software: No backdoors, no registration. Beta software.
- miniLock (<https://minilock.io/>) - Browser plugin for Google Chrome / Chromium to encrypt files using a secret passphrase. Easy to use. From the developer of Cryptocat.
- AES Crypt (<https://www.aescrypt.com/>) - Using a powerful 256-bit encryption algorithm, AES Crypt can safely secure your most sensitive files. For Windows, Mac, Linux and Android.
- DiskCryptor (<https://diskcryptor.net/>) - A full disk and partition encryption system for Windows including the ability to encrypt the partition and disk on which the OS is installed.

Self-contained Networks

If you are currently browsing the Clearnet (https://en.wikipedia.org/wiki/Surface_Web) and you want to access the Deep Web (https://en.wikipedia.org/wiki/Deep_Web) this section is for you.

I2P Anonymous Network

The Invisible Internet Project (I2P) is a computer network layer that allows applications to send messages to each other pseudonymously and securely. Uses include anonymous Web surfing, chatting, blogging and file transfers. The software that implements this layer is called an I2P router and a computer running I2P is called an I2P node. The software is free and open source and is published under multiple licenses.

Website: geti2p.net
(<https://geti2p.net/>)

OS: Windows, Mac, Linux, Android, F-Droid.

GUnet Framework

GUnet is a free



software framework for decentralized, peer-to-peer networking and an official GNU package. The framework offers link encryption, peer discovery, resource allocation, communication over many transports (such as tcp, udp, http, https, wlan and bluetooth) and various basic peer-to-peer algorithms for routing, multicast and network size estimation.

Website: gnunet.org
(<https://gnunet.org/>)

OS: GNU/Linux, FreeBSD, NetBSD, OpenBSD, Mac, Windows.

The Freenet Project

Freenet is a



peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship. Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection.

Website: freenetproject.org
(<https://freenetproject.org/>)

OS: Windows, Mac, Linux.

Worth Mentioning

- Tor Project (<https://www.torproject.org/>) - Provides anonymity to websites and other servers. Servers configured to receive connections only through Tor are called hidden services.
- RetroShare (<http://retroshare.sourceforge.net/>) - Open Source cross-platform, Friend-2-Friend and secure decentralised communication platform.

Decentralized Social Networks

If you are currently using Social Networks like Facebook, Twitter or Google+ you should pick an alternative here.

diaspora*



diaspora* is based on three key philosophies: Decentralization, freedom and privacy. It is intended to address privacy concerns related to centralized social networks by allowing users set up their own server (or "pod") to host content; pods can then interact to share status updates, photographs, and other social data.

Website: diasporafoundation.org
(<https://diasporafoundation.org/>)

Friendica



Friendica has an emphasis on extensive privacy settings and easy server installation. It aims to federate with as many other social networks as possible. Currently, Friendica users can integrate contacts from Facebook, Twitter, Diaspora, GNU social, App.net, Pump.io and other services in their social streams.

Website: friendica.com
(<http://friendica.com/>)

GNU social



While offering functionality similar to Twitter, GNU social seeks to provide the potential for open, inter-service and distributed communications between microblogging communities. Enterprises and individuals can install and control their own services and data. Notable public deployments are quitter.se (<https://quitter.se/>) and gnusocial.no (<https://gnusocial.no>).

Website: gnu.io
(<https://gnu.io/social/try/>)

Worth Mentioning

- Libertree (<http://libertreeproject.org/>) - A free, libre, open-source software which is intended to provide a way for people to create their own social network. Currently in an invitational alpha phase.

Related Information

- Delete your Facebook account (https://www.facebook.com/help/delete_account) - Direct link to delete your Facebook account without being able to reactivate it again.
- How To Permanently Delete A Facebook Account (<http://deletefacebook.com/>) - This guide will take you through a smooth and successful Facebook account deletion.

Domain Name System (DNS)

CloudDNS - Service

Free DNS,



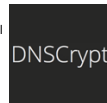
Managed DNS and DDoS Protected DNS hosting with included web redirects, mail forwards and Round-Robin load balancing. Instant updates in Europe, North America, Asia and Australia. CloudDNS have a self developed system for management and DNS synchronization. Every customer can see where his domain zone is up-to-date and running.

Website: [cloudns.net](https://www.cloudns.net/)
(<https://www.cloudns.net/>)

OS: Cross-platform.

DNSCrypt - Tool

A protocol for



securing communications between a client and a DNS resolver. The DNSCrypt protocol uses high-speed high-security elliptic-curve cryptography and is very similar to DNSCurve, but focuses on securing communications between a client and its first-level resolver.

Website: dnscrypt.org
(<http://dnscrypt.org/>)

OS: Windows, Mac, Linux, iOS with Jailbreak.

OpenNIC - Service



OpenNIC is an alternate network information center/alternative DNS root which lists itself as an alternative to ICANN and its registries. Like all alternative root DNS systems, OpenNIC-hosted domains are unreachable to the vast majority of the Internet. Only specific configuration in one's DNS resolver makes these reachable, and very few Internet service providers have this configuration.




Website: [opennicproject.org](http://www.opennicproject.org/)
(<http://www.opennicproject.org/>)

OS: Cross-platform.

Worth Mentioning

- Namecoin (<https://namecoin.info/>) - A decentralized DNS open source information registration and transfer system based on the Bitcoin cryptocurrency.

☞ Productivity Tools




<p>Etherpad</p>  <p>Etherpad is a highly customizable Open Source online editor providing collaborative editing in real-time. Etherpad allows you to edit documents collaboratively in real-time, much like a live multi-player editor that runs in your browser. Write articles, press releases, to-do lists, etc.</p> <p>Website: etherpad.org (http://etherpad.org/)</p> <p>OS: Windows, Mac, Linux.</p>	<p>EtherCalc</p>  <p>EtherCalc is a web spreadsheet. Data is saved on the web, and people can edit the same document at the same time. Changes are instantly reflected on all screens. Work together on inventories, survey forms, list management, brainstorming sessions..</p> <p>Website: ethercalc.net (https://ethercalc.net/)</p> <p>OS: Windows, Mac, GNU/Linux, FreeBSD, Browser.</p>	<p>ProtectedText</p>  <p>ProtectedText is an open source web application. It encrypts and decrypts text in the browser, and password (or it's hash) is never sent to the server - so that text can't be decrypted even if requested by authorities. No cookies, no sessions, no registration, no users tracking.</p> <p>Website: protectedtext.com (https://www.protectedtext.com/)</p> <p>OS: All Browsers.</p>
---	---	---

Worth Mentioning

- [dudle \(https://dudle.inf.tu-dresden.de/privacy/\)](https://dudle.inf.tu-dresden.de/privacy/) - An online scheduling application, which is free and OpenSource. Schedule meetings or make small online polls. No email collection or the need of registration.
- [Turtli \(https://turtli.it/\)](https://turtli.it/) - Remember ideas, track research, share documents, or bookmark your favorite sites. Turtli makes it easy to organize your life and uses solid encryption to keep it all safe.

☞ PC Operating Systems

If you are currently using a operating system like Microsoft Windows or Apple Mac OS X you should pick an alternative here.

<p>Debian</p>  <p>Debian is a Unix-like computer operating system and a Linux distribution that is composed entirely of free and open-source software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian project.</p> <p>Website: debian.org (https://www.debian.org/)</p>	<p>Trisquel</p>  <p>Trisquel is a Linux-based operating system derived from Ubuntu. The project aims for a fully free software system without proprietary software or firmware and uses Linux-libre, a version of the Linux kernel with the non-free code (binary blobs) removed.</p> <p>Website: trisquel.info (http://trisquel.info/)</p>	<p>Qubes OS</p>  <p>Qubes is an open-source operating system designed to provide strong security for desktop computing. Qubes is based on Xen, the X Window System, and Linux, and can run most Linux applications and utilize most of the Linux drivers.</p> <p>Website: qubes-os.org (https://www.qubes-os.org/)</p>
--	---	--

Warning

- Don't use Windows 10 - It's a privacy nightmare

Worth Mentioning

- [OpenBSD \(http://www.openbsd.org/\)](http://www.openbsd.org/) - A project that produces a free, multi-platform 4.4BSD-based UNIX-like operating system. Emphasizes portability, standardization, correctness, proactive security and integrated cryptography.
- [Arch Linux \(https://www.archlinux.org/\)](https://www.archlinux.org/) - A simple, lightweight Linux distribution. It is composed predominantly of free and open-source software, and supports community involvement
- [Whonix \(https://www.whonix.org/\)](https://www.whonix.org/) - A Debian GNU/Linux based security-focused Linux distribution. It aims to provide privacy, security and anonymity on the internet. The operating system consists of two virtual machines, a "Workstation" and a Tor "Gateway". All communication are forced through the Tor network to accomplish this..

🔗 Live CD Operating Systems

<p>Tails</p> <p>Tails is a live operating system, that starts on almost any computer from a DVD, USB stick, or SD card. It aims at preserving privacy and anonymity, and helps to: Use the Internet anonymously and circumvent censorship; Internet connections go through the Tor network; leave no trace on the computer; use state-of-the-art cryptographic tools to encrypt files, emails and instant messaging.</p> <p>Website: tails.boum.org (https://tails.boum.org/)</p>	<p>KNOPPIX</p> <p>Knoppix is an operating system based on Debian designed to be run directly from a CD / DVD (Live CD) or a USB flash drive (Live USB), one of the first of its kind for any operating system. When starting a program, it is loaded from the removable medium and decompressed into a RAM drive. The decompression is transparent and on-the-fly.</p> <p>Website: knopper.net (http://www.knopper.net/knoppix/)</p>	<p>Puppy Linux</p> <p>Puppy Linux operating system is a lightweight Linux distribution that focuses on ease of use and minimal memory footprint. The entire system can be run from RAM with current versions generally taking up about 210 MB, allowing the boot medium to be removed after the operating system has started.</p> <p>Website: puppylinux.org (http://puppylinux.org/)</p>
---	---	---

Worth Mentioning

- JonDo Live-CD (<https://anonymous-proxy-servers.net/en/jondo-live-cd.html>) - A secure, pre-configured environment for anonymous surfing and more. It is based on Debian GNU/Linux. The live system contains proxy clients for JonDonym, Tor Onion Router and Mixmaster remailer. JonDoFox is a pre-configured browser for anonymous web surfing and TorBrowser is installed too..
- Tiny Core Linux (<http://distro.ibiblio.org/tinycorelinux/>) - A minimal Linux operating system focusing on providing a base system using BusyBox and FLTK. The distribution is notable for its size (15 MB) and minimalism, with additional functionality provided by extensions.

🔗 Mobile Operating Systems

<p>CyanogenMod</p> <p>CyanogenMod is an open-source operating system for smartphones and tablets, based on Android. It is developed as free and open source software based on the official releases of Android by Google.</p> <p>Website: cyanogenmod.org (http://www.cyanogenmod.org/)</p>	<p>Firefox OS</p> <p>Firefox OS is a kernel-based open-source operating system for smartphones and tablet computers and is set to be used on smart TVs. It is being developed by Mozilla.</p> <p>Website: mozilla.org (http://mozilla.org/firefox/os)</p>	<p>Ubuntu Touch</p> <p>Ubuntu Touch is a mobile version of the Ubuntu operating system developed by Canonical UK Ltd and Ubuntu Community. It is designed primarily for touchscreen mobile devices such as smartphones and tablet computers.</p> <p>Website: ubuntu.com (http://www.ubuntu.com/phone)</p>
---	--	--

Worth Mentioning

- Replicant (<http://www.replicant.us/>) - A free and open source operating system based on the Android, which aims to replace all proprietary Android components with their free software counterparts.

🔗 Open Source Router Firmware

<p>OpenWrt</p> <p>OpenWrt is an operating system (in particular, an embedded operating system) based on the Linux kernel, primarily used on embedded</p>	<p>pfSense</p> <p>pfSense is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a computer to make a dedicated firewall/router for a</p>	<p>LibreWRT</p> <p>LibreWRT is a GNU/Linux-libre distribution for computers with minimal resources, such as the Ben Nanonote, ath9k</p>
---	---	--

devices to route network traffic. The main components are the Linux kernel, util-linux, uClibc and BusyBox. All components have been optimized for size, to be small enough for fitting into the limited storage and memory available in home routers.

Website: openwrt.org
(<https://openwrt.org/>)

network and is noted for its reliability and offering features often only found in expensive commercial firewalls. pfsense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint.

Website: [pfsense.org](https://www.pfsense.org/)
(<https://www.pfsense.org/>)

based wifi routers, and other hardware that respects your freedom with emphasis on free software. It is used by the Free Software Foundation on their access point and router which provides network connectivity to portable computers in their office.

Website: librewrt.org
(<http://librewrt.org/>)

Worth Mentioning

- **OpenBSD** (<http://www.openbsd.org/>) - A project that produces a free, multi-platform 4.4BSD-based UNIX-like operating system. Emphasizes portability, standardization, correctness, proactive security and integrated cryptography.
- **DD-WRT** (<http://www.dd-wrt.com/>) - A is Linux-based firmware for wireless routers and wireless access points. It is compatible with several models of routers and access points.

🔗 Quotes

Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

— Edward Snowden on *reddit* (https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2)

The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards. I don't want to live in a society that does these sort of things... I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under.

— Edward Snowden in *The Guardian* (<http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why>)

We all need places where we can go to explore without the judgmental eyes of other people being cast upon us, only in a realm where we're not being watched can we really test the limits of who we want to be. It's really in the private realm where dissent, creativity and personal exploration lie.

— Glenn Greenwald in *Huffington Post* (http://www.huffingtonpost.com/2014/06/20/glenn-greenwald-privacy_n_5509704.html)

🔗 Recommended Privacy Resources

- **ipleak.net** (<http://ipleak.net/>) - IP/DNS Detect - What is your IP, what is your DNS, what informations you send to websites.
- **Surveillance Self-Defense by EFF** (<https://ssd.eff.org/>) - Guide to defending yourself from surveillance by using secure technology and developing careful practices.
- **PRISM Break** (<https://prism-break.org/>) - We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services.
- **Security in-a-Box** (<https://securityinabox.org/>) - A guide to digital security for activists and human rights defenders throughout the world.
- **The Ultimate Privacy Guide** (<https://www.bestvpn.com/the-ultimate-privacy-guide/>) - Excellent privacy guide written by the creators of the bestVPN.com website.
- **IVPN Privacy Guides** (<https://www.ivpn.net/privacy-guides>) - These privacy guides explain how to obtain vastly greater freedom, privacy and anonymity through compartmentalization and isolation.
- **AlternativeTo.net** (<http://alternativeto.net/?license=open-source&platform=self-hosted&sort=likes>) - Great collection of open source online and self-hosted software sorted by likes.
- **Keybase.io** (<https://keybase.io/>) - Get a public key, safely, starting just with someone's social media username.
- **Security Now!** (<https://www.grc.com/securitynow.htm>) - Weekly Internet Security Podcast by Steve Gibson and Leo Laporte.
- **Reset The Net - Privacy Pack** (<https://pack.resetthenet.org/>) - Help fight to end mass surveillance. Get these tools to protect yourself and your friends.
- **SecureDrop** (<https://securedrop.org/>) - An open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. It was originally created by the late Aaron Swartz and is currently managed by Freedom of the Press Foundation.

🔗 Spread the word and help your friends



Copy URL and Description

www.privacytools.io - encryption against global mass surveillance

For easy copy and paste. Share this text snippet.

Participate with suggestions and constructive criticism

(<http://www.reddit.com/r/privacytoolsIO/>)

It's important for a website like privacytools.io to be up-to-date. Keep an eye on software updates of the applications listed here. Follow recent news about providers that are recommended. We try our best to keep up but we're not perfect and the internet is changing fast. If you find an error, or you think a provider should not be listed here, or a qualified service provider is missing or a browser plugin is not the best choice anymore and anything else... **Talk to us please.** This is a community project and we're aiming to deliver the best information available for a better privacy.



Here is what you can do:

Make suggestions on reddit: <https://www.reddit.com/r/privacytoolsIO/> (<https://www.reddit.com/r/privacytoolsIO/>)

Follow on Twitter: <https://twitter.com/privacytoolsIO> (<https://twitter.com/privacytoolsIO>)

View and edit our website source code on GitHub: <https://github.com/privacytoolsIO/privacytools.io> (<https://github.com/privacytoolsIO/privacytools.io>)

Thank you for participating. This projects needs you.

No Ads, No Google Analytics, No Affiliates, No Cross-Site Requests



Creative Commons (<http://creativecommons.org/licenses/by-sa/4.0/>)



kopimi (copyme) (<http://www.kopimi.com/>)



Donate: ([donate.html](https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=7MPR5TEA9KJZY))

1N6heMWD34ARyApkRmNv7V7NzQFYvgC4dg or use PayPal. (https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=7MPR5TEA9KJZY)

privacytools.io is a socially motivated website that provides information for protecting your data security and privacy. never trust any company with your privacy, always encrypt.