

How to protect your privacy on the internet

This document provides a non-exclusive and not prioritized list of software tools and services that help citizens to protect their privacy in Internet.

Disk Encryption

- DiskCryptor - https://diskcryptor.net/wiki/Main_Page ¹
- tcNext - <https://truecrypt.ch/> ^{1,2,3}
- CipherShed - <https://ciphershed.org/> ^{1,2,3}
- FileVault - <http://support.apple.com/en-us/HT4790> ²
- BitLocker – <http://windows.microsoft.com/en-us/windows7/products/features/bitlocker> ¹
- GnuPG - <https://gnupg.org/> ^{1,2,3,4}

Encryption of Communication Channel

- HTTPS Everywhere - <https://www.eff.org/https-everywhere> ^{7,8,9}

Email

- Prism - <http://prismproof.org/index.html> ^{1,2,3}
- BitMessage - https://bitmessage.org/wiki/Main_Page ^{1,2,3}
- Sendinc - <https://www.sendinc.com/> ^{*}
- Enigmail - <https://enigmail.net/home/index.php> ^{1,2,3,4}
- Mailvelope - <https://www.mailvelope.com/> ^{7,8}
- GnuPG - <https://www.gnupg.org/> ^{1,2,3,4}
- Startmail - <https://live.startmail.com/> ^{*}
- GPG Tools - <https://gpgtools.org/> ²
- iPGmail - <https://ipgmail.com/> ⁶
- And You And I - <https://andyouandiapp.wordpress.com/> ⁶
- oPenGP - <https://itunes.apple.com/us/app/opengp/id414003727?mt=8> ⁶

Voice (and Video) Communication

- Cellcrypt - <http://cellcrypt.com/> ^{4,5,6}
- Celltrust - <http://www.celltrust.com/> ^{4,6}
- OSTN - <https://ostel.co/> ^{*}
- Omnisec - <http://www.omnisec.ch> ^{*}
- Seecrypt - <https://www.seecrypt.com/> ^{1,4,5,6}
- SilentPhone - <https://silentcircle.com> ^{4,6}
- Redphone - <https://whispersystems.org/> ⁴
- Jitsi - <https://jitsi.org/> ^{1,2,3}
- Tox - <https://tox.im/> ^{*}

Web Browsing

TOR – <https://www.torproject.org/>^{1,2,3} (Has recently been compromised. Refer to TOR Blog for more information)
I2P – <https://geti2p.net>^{1,2,3,4}
Blur – <https://dnt.abine.com> *
Disconnect – <https://disconnect.me/>^{1,2,4,6}
NoScript – <http://noscript.net/>⁷
Orweb – <https://play.google.com/> (Search for application Orweb)⁴
Onion Browser – <https://itunes.apple.com/us/app/onion-browser/id519296448?mt=8>⁶

Chat / IM

TorChat – <https://github.com/prof7bit/TorChat/downloads>^{1,3}
Pidgin – <https://pidgin.im/>^{1,2,3}
Adium – <https://www.adium.im/>²
MiOTR – <http://code.google.com/p/mirottr/>¹
Cryptocat – <https://crypto.cat/>^{2,6,7,8,9,10}
Jitsi - <https://jitsi.org/>^{1,2,3}
ChatSecure - <https://itunes.apple.com/us/app/opengp/id414003727?mt=8>⁶

Search Engines

DuckDuckGo - <https://duckduckgo.com/> *
Ixquick - <https://ixquick.com/> *
StartPage – <https://startpage.com/> *

Operating Systems

Qube OS - <https://qubes-os.org/>
OpenBSD – <http://www.openbsd.org/>
TAILS - <https://tails.boum.org/>

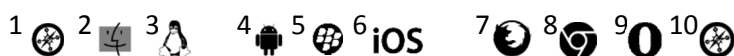
Install perimeter security – firewalls and antivirus

Apply software and security updates regularly – setup automatic updates if possible

Use strong passwords – more than 8 chars using a mix of alphanumeric and special symbols

Do not open unknown mail attachments and do not follow suspicious web links

NEVER reveal your passwords or bank details to third parties



This document is an annex to the STOA Study on Mass Surveillance (PE 527.509) published in January 2015. The study and all its annexes can be found at <http://www.europarl.europa.eu/stoa/>

© European Union, 2015.

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.