



Aurea ✓
@AureaLibe



[Guide] How to escape Chat Control and the monitoring of your private messages

The European Parliament has adopted Chat Control. Scanning our private messages is now authorized in the Union, in the name of "protecting children." A majority of MEPs voted against the text, but, due to a procedural rule, an absolute majority would have been required to reject it. This was not achieved. Mass surveillance has been eliminated. Since my beginnings, I have defended three simple things: the People, Freedom, and privacy.

So here's a guide to take action. This article is a shorter version of my full guide. You can find the complete version on a dedicated website here:

exitchatcontrol.org

I will give you all the tools to take action, with concrete steps, in order, from the simplest to the most advanced.

The most dangerous version of Chat Control relies on "client-side scanning": software that reads your messages directly on your phone, before they are encrypted.

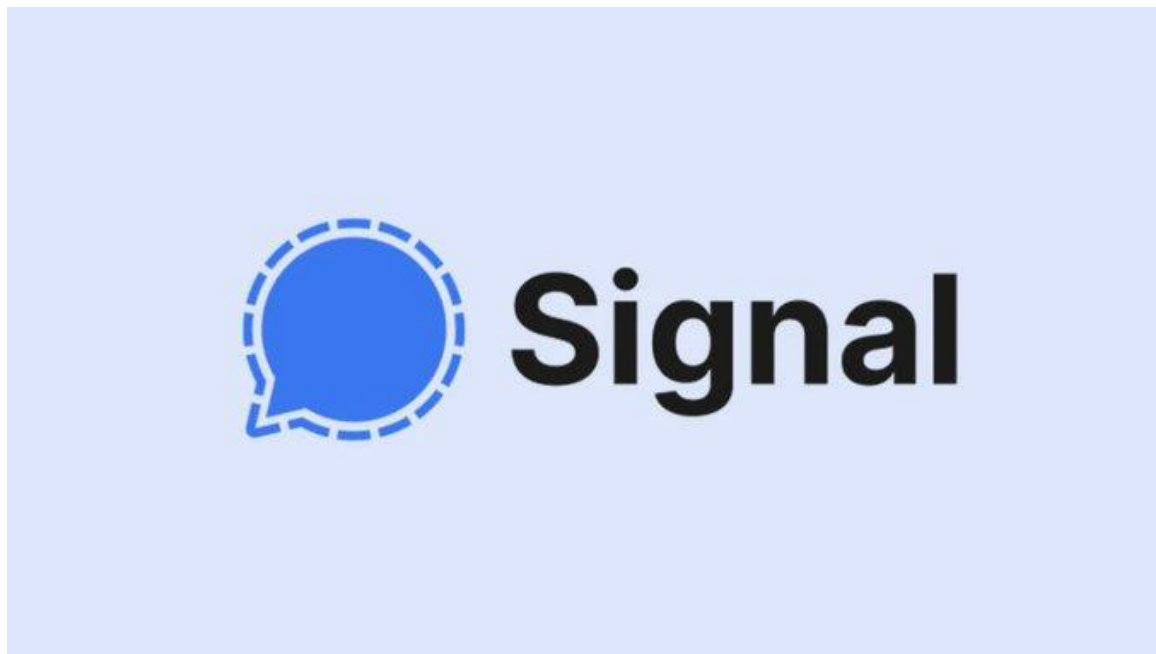
Consequently, a VPN alone, or simple encryption, will not be enough to protect against it.

Each of the methods that follow will protect you a little more. You don't have to do everything at once. But resistance begins with individual actions, and individual responsibility begins with education, and I'm going to help you with that.

What will truly protect you is switching to free software that rejects this spyware, regaining control of your device, and thus becoming sovereign over the tools you use.

Step 1: Change your email provider (the most urgent action)

This is the first thing you should do, the one that protects you the fastest. Quit WhatsApp, Messenger, and Telegram and install Signal.



It's a messaging service as easy to use as WhatsApp, but end-to-end encrypted by default, run by a non-profit foundation, and its team has promised to leave Europe rather than install a scan of your messages.

Go to

signal.org

Install the app, confirm your number, then in Settings > Privacy, create a username to hide your number.

If you want to go further, SimpleX Chat (

simplex.chat

) doesn't ask for a number, email, or any other identifier. Nobody, not even the servers, knows who is talking to whom. I can also recommend, in the same vein, Session (

getsession.org

). Most importantly: get your contacts to install Signal. Encrypted messaging is useless if you're the only one using it. *To learn more, the complete guide is [available here](#).*

Step 2: Quit Gmail

Gmail reads your emails and is based in the United States, under its jurisdiction. Leaving it is a huge gain for very little effort. Create an account on Proton Mail (proton.me), based in Switzerland and encrypted. The free plan is all you need to get started. When you sign up, use the "Easy Switch" tool to import your old messages and contacts, set up a forward from Gmail, and notify your contacts of your new address.



An equally solid alternative that I recommend: Tuta (tuta.com), German, completely free.
To learn more, the complete guide is [available here](#).

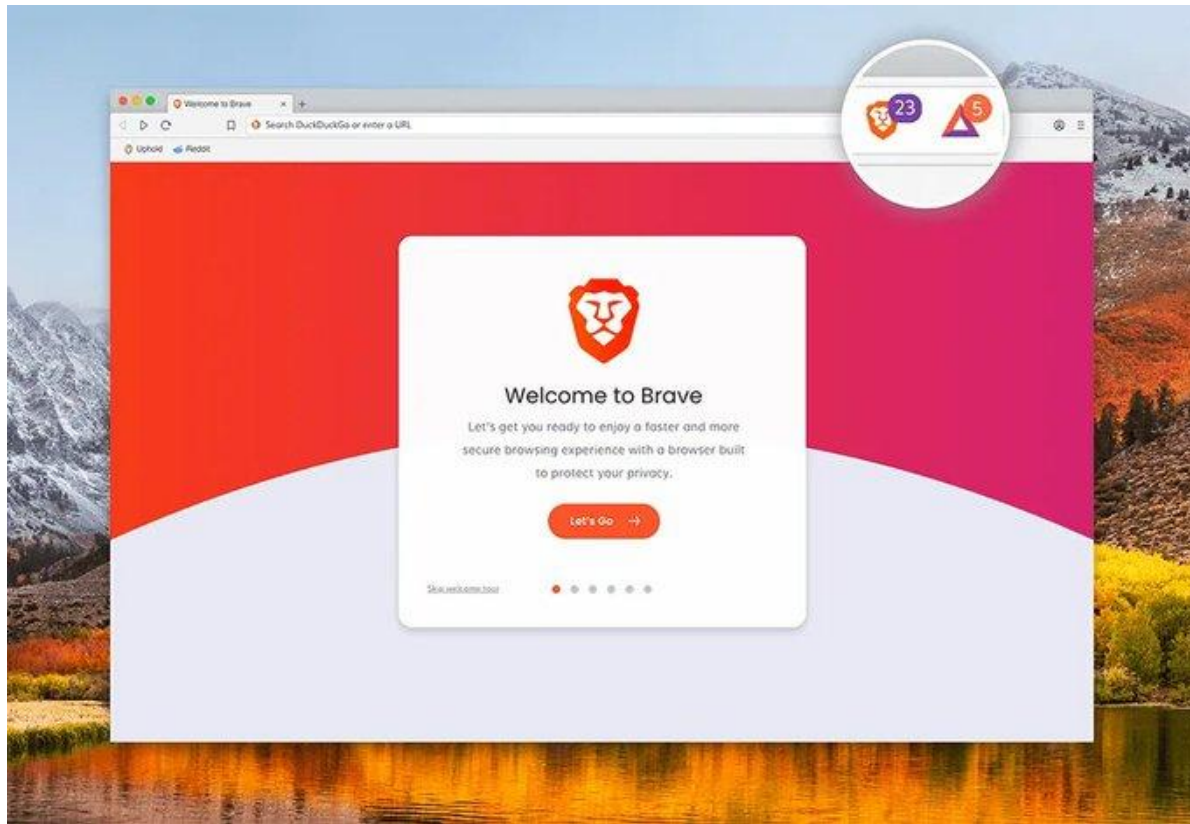
Step 3: Change your browser, your search engine, and get away from Google

Chrome is an advertising spy, and Google records every single one of your searches. We're replacing both.

For a painless switch, install Brave (brave.com)

), the internet browser of [@BrendanEich](#)

He worked on the first internet browser, invented JavaScript, the language used everywhere on the internet, and co-founded the Mozilla Firefox browser.



Brave is like Chrome, but without the spyware. It blocks ads and trackers by default, blocks YouTube ads, and even includes one-click access to Tor. It's a privacy-focused browser that will keep your data safe from Google's spying.

As a free alternative, I can recommend Librewolf (librewolf.net)

) However, I would not recommend Firefox, whose leader has made some statements contrary to the protection of privacy. Finally, change your browser's default search engine, whether on your computer or smartphone. I recommend using Brave's search engine, Brave Search (search.brave.com)

), and, as an alternative, DuckDuckGo (duckduckgo.com).

To learn more, the complete guide is [available here](#).

Step 4: Use a VPN

A VPN doesn't protect you from scanning your device, but it masks your IP address from your internet service provider and gives you access to sites that require ID. This will be essential when anonymity becomes a thing of the past.

I recommend **Mullvad** (mullvad.net)

): no email, no name, just an account number, an audited no-logs policy, and a fixed price.



In concrete terms: 1. Go to

mullvad.net

(If the site is blocked for you, open it via the Tor browser or its .onion address).

2. Click on "Generate an account number". **Save this number** in your password manager and never share it: it is your only key.

3. Pay. If your bank card works, keep it simple. If you want complete anonymity, pay with cryptocurrency: click on "Create a one-time payment address" and send the amount from your wallet. Monero is the most private. The detailed purchase tutorial (Bitcoin, Monero via swap) is in this comprehensive guide:

<https://x.com/AureaLibe/status/2016126634235953211>

.

4. Download the application on

mullvad.net/download

Enter your number and connect to a server outside the European Union. Activate the "kill switch".

To learn more, the complete guide is [available here](#).

Step 5: Secure your accounts

A unique and strong password per service is the basis of all security.

Install Bitwarden (

bitwarden.com

), free and open source. Create a long master password (a phrase), install the extension and the application, and let it save and then replace your old passwords.



It's important to store your passwords in open-source software and not entrust them to Google or Apple. Your passwords grant access to your entire life. Just as you wouldn't give your house keys to strangers, it's your responsibility to do the same with your passwords.

In addition, a password manager allows you to use a different password on each site, which strengthens your privacy and limits the risk of hacking.

Next, **enable two-** factor authentication on your important accounts, using an application like Aegis (

getaegis.app

) or Auth Entity (

ente.com

), and never by SMS (SMS is vulnerable to SIM card hacking).

To learn more, the complete guide is [available here](#).

Step 6: Take back control of your devices

This is the point that many forget: we encrypt our messages but we keep a system that spies on us.

On your computer, switch to **Linux** . It's free, it doesn't spy on you, and it's much simpler than you think. Recent distributions, especially those with the GNOME and KDE desktop environments, are very intuitive. Software is readily available, and even for video games, there are distributions with everything you need pre-installed, such as CachyOS (

cachyos.org

) or Steam OS (

store.steampowered.com/steamos

On my gaming computer, Linux has become my default choice. To begin, Linux Mint (

linuxmint.com

) is the simplest distribution and the closest to Windows.



On a phone, the most robust solution is GrapheneOS (

grapheneos.org

). This is a de-Googled and hardened version of Android that can be installed on a Google Pixel in a few clicks from a computer.



This is the real solution if your phone ever tries to scan you or spy on your conversations. Because the only real way to bypass this type of surveillance is to install a version of Android that isn't controlled by Google.

To learn more, the complete guide is [available here](#).

Step 7: To go further

If you want to take sovereignty to the extreme: use **Tor** to dissociate your activity from your IP address, host your own services with **YunoHost** or **Umbrel**, run **artificial intelligence locally** instead of sending your thoughts to ChatGPT, and for those most at risk, learn the rules of anonymity. Everything is detailed, step by step, in the complete guide available here: exitchatcontrol.org

Conclusion

Changing tools is an act of individual responsibility, unique to each person, which allows one to refuse illegitimate mass surveillance.

Encrypting your data protects your privacy. Self-hosting frees you from the surveillance of tech companies. Taking back control of your tools makes you ungovernable and sovereign.

The fight is political. Support the organizations that oppose it, such as the initiative fightchatcontrol.eu

And write to your elected officials. That's what almost brought down Chat Control.

But since the solution will probably not come through the ballot box or the European Parliament, it is everyone's responsibility to win their freedom and protect their privacy with all the tools available on the Internet. *The complete guide, with each tool explained and installed step by step, from citizen to whistleblower, is here*

exitchatcontrol.org

Save it, share it, and get your loved ones to migrate it.

This article will be updated as the situation evolves.