

The AI Privacy Policy Guide

Introduction

With rapidly growing tech greed, the daily consumer has turned to be a free data extraction tool for which most governments don't yet have a solution to. Most companies have recently activated AI to scan messages, save and collect biometric data (scanning photos, lives , videos, video chats, etc.) in order to train their models. If you strongly object to any of these practices – you can find some valuable information in this guide on how to turn off hidden AI features from your daily internet activity. I've also included some alternatives for safer internet space that offer the same experience ,if not – better.

1. Gmail

- Settings -> See all settings -> search for '*smart features*' -> Uncheck "*Turn on smart features in Gmail, Chat, Meet*"
- Right below it click "*Manage Workspace smart feature settings*" and turn off the 2 toggles

If you feel untrustworthy of Gmail , you can use any of these alternatives:

Proton – 1GB free space, E2EE (safe communication)

Tuta Mail – German, 1GB free space, E2EE, doesn't log IP, no phone for sign-up

Zoho Mail – ad-free , privacy first, custom domain

2. Google accounts

- Go to your Google account -> <https://myaccount.google.com/> -> search for "**Web & App Activity**" -> turn off and delete your activity collected by now
- Turn off **Timeline activity** if you don't want your data from Google Maps to be tracked and saved
- Go to **My Ads Center** and toggle off personalization
- If needed : Click **Google partner settings** and toggle off "... save data in your Google Account from sites and apps that partner with Google..."
- **Gemini Apps Activity** - > Turn off '*Keep Activity*'

Alternatives:

Tuta - German , mail, calendar, contacts with no tracking ads

Proton - Switzerland, mail, calendar ,drive ,password manager ,zero-access encryption

Mailbox.org – Applies strict EU regulations ,cloud storage, documents, mail

Cons:

No OAuth

3. Instagram

Profile -> Settings -> Privacy center -> Look below "*Privacy topics*" -> AI at Meta -> "*Right to object..*" -> "*information you've shared on Meta Products*" -> scroll down -> Submit objection

Alternative:

Pixelfed – decentralized ,open-source, photo sharing platform, mimics “old instagram”

Spacehey – decentralized, mySpace mock

4. Messaging

Discord, Snapchat, Instagram, X(Twitter), TikTok, Telegram, Slack, Microsoft Teams

DON'T use E2EE meaning that all of your messages, texts, images, videos and audios are saved as unprotected plain raw data on the servers of the corporations. The reason they give is “law enforcement”, but there are ways to gather evidence without *breaking the envelope seal* for every user on the platform.

Alternatives for everyday messaging

Top choices:

Signal – Non-profit, decentralized, E2EE, 0 metadata collection

Element – For big groups/organizations , uses Matrix (decentralized network protocol), privacy focused, doesn't required a phone number ,but just a username

Briar – P2P , no cloud centered server, messages sync between devices via Tor, Bluetooth or Wi-Fi, works even if the internet grid is down, used by activists and journalists

Threema – complies with strict EU policy, no phone number or email, no metadata collection, secure servers in Switzerland

Session – Impossible to track your IP or physical address , no metadata collection, decentralized onion-routing

Global choices with compromises:

WhatsApp – Signal encryption, but a con: heavy metadata collection (who,when,where,etc.)

Viber – E2EE, also tracks metadata to push ads on the platform