

# Los van BigTech

*Een praktische overstapgids*



# Los van BigTech overstapgids

## Overstappen van BigTech naar privacyvriendelijke technologie

De moderne digitale wereld draait op populaire oplossingen die vaak grote privacyrisico's en afhankelijkheid van Big Tech met zich meebrengen. Gelukkig bestaan er voor alles Europese en/of open-source, privacyvriendelijke alternatieven waarmee je weer meer controle krijgt over je eigen gegevens.

Deze handleiding helpt je stap voor stap, in 12 thema's, om praktisch en haalbaar over te stappen naar een veiliger digitaal systeem. Het gaat niet om alles in één keer veranderen, maar om geleidelijk slimme keuzes maken die bij jouw leven passen. Het doel is meer regie over je data, minder afhankelijkheid en minder surveillance, terwijl je gewoon blijft werken op je laptop en smartphone.

Je hoeft niet technisch te zijn: begin met het onderdeel dat jou het meeste oplevert. Elke stap maakt je leven een beetje vrijer. Kies bij voorkeur voor meerdere systemen, apps en aliases in plaats van alles op één plek, want één systeem is kwetsbaar: het kan makkelijker data verzamelen, verkocht worden, gevolgd worden of in één keer worden uitgezet.

### Los van BigTech in 12 stappen:

1. Smartphone besturingssysteem
2. Computer besturingssysteem
3. Browsers en zoekmachines
4. Netwerkbeveiliging
5. Virusscanners en Internetbeveiliging
6. Office en dataopslag
7. E-mail
8. Chat en videobellen
9. AI-tools
10. Wachtwoordbeheer
11. Encryptie
12. Andere services vervangen

## 1. Smartphone besturingssysteem

Je smartphone is het meest gevolgde apparaat in je leven. Een privacygericht besturingssysteem in plaats van standaard iOS, Android of Windows maakt daarom het grootste verschil in of en hoeveel data je deelt, hoeveel tracking er plaatsvindt en hoe goed je toestel tegen misbruik is beschermd.

Er zijn op dit moment twee realistische richtingen:

- GrapheneOS op een ontgrendelde Google Pixel
- LinuxOS op een Linux smartphone zoals Fairphone of Jolla.

GrapheneOS is technisch gezien de meest veilige optie. Je vervangt Android volledig door GrapheneOS op een moderne, ontgrendelde Pixel. Dat is ironisch, want je gebruikt Google-hardware om juist van Google af te komen, en voor wie wantrouwig is voelt dat dubbel. Koop daarom bij voorkeur een refurbished Pixel, zodat je Google niet direct steunt. Het wordt afgeraden om een Google Pixel met vooraf geïnstalleerde GrapheneOS te gebruiken aangezien dan onduidelijk is wat er nog meer op is geïnstalleerd. De installatie vraagt technische handelingen, maar is goed te doen en daarna werkt het toestel net als Android, maar met strengere beveiliging, app-isolatie en maximale prestaties. Op Graphene.org vind je een duidelijke handleiding (zie ook bijlage 1). Hopelijk komt er binnenkort een samenwerking tussen Motorola en GrapheneOS waardoor de installatie al is geregeld.

Linux telefoons met het Linux OS vooraf geïnstalleerd, zoals een Fairphone met /e/OS of Sailfish OS van Jolla werken meteen uit de doos, zijn duurzaam en repareerbaar, maar vragen wat gewenning en leveren iets in op pure beveiliging en prestaties.

Een praktische tip is om tijdelijk twee smartphones te gebruiken. De-google je oude toestel zoveel mogelijk en gebruik je "privacyphone" voor dagelijks gebruik zonder Big Tech. Zo kun je rustig overstappen, wennen aan alternatieven en stap voor stap meer controle krijgen over je digitale leven, zonder alles in één keer te hoeven omgooien.

## 2. Computer besturingssysteem

De volgende stap naar digitale vrijheid is wijzigend van je besturingssysteem. Dat bepaalt wie controle over jouw data heeft. Windows en macOS zijn dure gesloten BigTech systemen die bekendstaan om dataverzameling, telemetrie en toenemende afhankelijkheid van hun eigen diensten. Wie daar echt van los wil komen, kiest voor Linux.

Linux is open source, community-gedreven en voor altijd gratis. De broncode is openbaar en wordt door duizenden ontwikkelaars gecontroleerd en verbeterd. Dat betekent: geen ingebouwde advertenties, geen verplichte accounts en geen stille datastromen naar Big Tech. Bovendien is Linux in de praktijk veiliger: er is veel minder malware, en fouten worden sneller ontdekt en opgelost, wachtwoordgebruik bij installatie van programma's. Je krijgt ook iets terug wat zeldzaam is geworden: echte controle over je eigen computer, zonder kunstmatige beperkingen. Voor beginners is Linux Mint een aanrader door de stabiliteit en een vertrouwd uiterlijk, Ubuntu is wat breder ondersteund en erg goed gedocumenteerd en Fedora is iets technischer, maar heeft extra focus op privacy en vernieuwing.

Je kunt Linux vrijblijvend uitproberen via een USB-stick, zonder iets te installeren. Bevalt het, dan kun je kiezen om het van de USB-stick te installeren en volledig over te stappen of te dual-booten naast je huidige systeem. (zie ook bijlage 2).

Ik raad in het begin gebruik van twee systemen aan. Dan werk je in je vertrouwde omgeving op je oude systeem als je wilt, en poog je zo veel mogelijk daarbuiten op Linux te doen. Ontgoogle en ontkoppel wel ook je oude systeem met de volgende stappen. Hiermee maak je de overgang naar Linux kleiner en zet je toch stappen richting minder afhankelijkheid, minder surveillance en meer digitale autonomie.

### 3. Browsers en zoekmachines

Browsers en zoekmachines zijn de poortwachters van je digitale leven. Elke klik, elke zoekopdracht en elke website die je bezoekt kan worden gevolgd, geanalyseerd en gebruikt om een profiel van je te bouwen. De standaardcombinaties Google met Chrome en Microsoft met Edge werken soepel, maar je betaalt een hoge prijs in de vorm van jouw privacy. Daarom is het vermijden of verwijderen van standaardbrowsers en zoekmachines als Google Chrome en Microsoft Edge en "easy sign in with Google/Microsoft" één van de meest effectieve plekken om los te komen van BigTech.

Als dagelijkse browser raad ik Vivaldi aan: een Noorse browser met veel mogelijkheden om instellen, zoals sterke privacy-opties aan te zetten en bijzonder in deze tijd zoeken zonder ingebouwde AI of advertentietracking. Voor situaties waarin je maximale anonimiteit wilt, is de Tor Browser geschikt, al is die merkbaar trager. Ook LibreWolf, Firefox, Mullvad, Qwant en Zen Browser zijn goede, privacyvriendelijke alternatieven. Voor zoeken vervang je Google door Startpage, Qwant of DuckDuckGo.

Je kan het ook technisch ingewikkelder kan je SearXNG of Metager.org gebruiken. Vooral Mojeek, Startpage en Qwant bouwen geen persoonlijk profiel van je en volgen je niet over het web. Je krijgt bij Mojeek de meeste privacy maar zoekresultaten vind je vanuit hun index. Wil je meer gebruikelijke zoekresultaten dan werkt Startpage of Qwant beter maar heeft iets minder privacy. Kies in de Vivaldi browser instellingen tracker-blokkering aan, zet third-party cookies uit en verwijder automatisch cookies. Overweeg eventueel een goede content-blocker zoals uBlock Origin voor extra rust en snelheid.

Met alleen de Vivaldi browser met standaard settings win je direct een enorme hoeveelheid privacy terug, zonder dat je inlevert op enig gebruiksgemak. Het is de kleinste stap, met een groot effect.

### 4. Netwerkbeveiliging

Een erg belangrijke maar wat technischere stap is om de beveiliging van je netwerk op orde te krijgen. Via BigTech lekt een hoop data en als je je voordeur open laat kan je ongenode gasten verwachten. Een firewall, DNS, VPN en je router bepalen of en wie jouw dataverkeer kunnen bepalen of inzien. Met een paar bewuste keuzes kun je je privacy en veiligheid enorm verbeteren, zonder dat het heel erg ingewikkeld hoeft te worden.

Firewalls vormen de bewaker aan de poort. Ze zorgen ervoor dat ongewenste verbindingen van buitenaf worden tegengehouden en dat apps niet zomaar kunnen "meeluisteren" of naar buiten communiceren. Je router heeft meestal al een basis-firewall die inkomend verkeer blokkeert, en ook je computer en smartphone hebben een ingebouwde firewall. Laat die altijd aan staan. Linux en GrapheneOS hebben ook goede firewalls. Voor de meeste mensen is de standaardinstelling voldoende, maar het bewust aan laten, of zo vaak mogelijk op de hoogste beveiliging laten staan en het up-to-date houden is een simpele en effectieve veiligheidslaag.

DNS werkt als het telefoonboek van internet: elke website die je bezoekt wordt eerst "opgezocht". Standaard loopt dit vaak via je internetprovider en de BigTechbedrijven. Zij krijgen zo inzicht in al je surfgedrag. Daarom is het verstandig een privacyvriendelijke DNS te gebruiken, zoals DNS4EU, Quad9 of AdGuardDNS of een vergelijkbaar alternatief. Zo voorkom je dat je zoekgedrag onnodig wordt gelogd of wordt gemanipuleerd. Je kunt maar een DNS-dienst tegelijk gebruiken of ze om en om per apparaat, browser of netwerklaag gebruiken. dns.adguard-dns.com is een goede optie.

Een VPN versleutelt al je internetverkeer en verbergt je IP-adres voor websites en netwerken. Dat is heel belangrijk op publieke wifi, wat je eigenlijk echt moet vermijden, aangezien meekijken of misbruik dan veel eenvoudiger is. VPN aanbieder met een goede reputatie zijn Proton VPN, Mullvad of Bitdefender VPN. Vermijd gratis VPN's, dan betaal je namelijk weer met je data. Tot slot is je router de poort naar het internet. Zorg voor actuele firmware van je router en een sterk wifi-wachtwoord voor een veiliger netwerk en het advies is om je VPN ook op je router te installeren. Samen zorgen firewalls, firmware, DNS, VPN ervoor dat je netwerk veiliger onder jouw controle blijft en pak je op netwerkniveau weer regie over je digitale leven.

## 5. Virusscanners en internetbeveiliging

Als je per ongeluk toch te maken krijgt met virussen, malware en andere internetdreigingen dan is een "internet security"-pakket op Windows of MacOS aan bevelen, zoals Bitdefender, ESET, F-Secure en Total AV. Op Linux en macOS zijn van nature minder aantrekkelijk doelwit voor malware dan Windows.

Linux is de kans op infectie kleiner daar voldoet open source ClamAV. Het aandeel echte Linux-malware is klein, mede door het systeemontwerp en de kleinere gebruikersgroep. Dat betekent dat de kans op een klassiek virus voor thuisgebruik veel lager is. Daarom draaien de meeste Linux-gebruikers geen virusscanner. ClamAV is vooral handig om bestanden te controleren die je met Windows-gebruikers deelt.

Op smartphones is het risico op klassieke virussen klein; het echte gevaar zit in malafide apps en misleiding. Daar helpt gezond verstand meer dan nog een scanner. Installeer alleen uit betrouwbare bronnen en houd alles up-to-date. En bedenk dat kritisch gedrag doet vaak veel meer voor je veiligheid én privacy dan zware security-pakketten.

## 6. Office en dataopslag

Voor je Office-, cloud- en datakeuzes geldt één simpele waarheid: hier ligt je leven opgeslagen. Wie dit beheert, heeft macht over je foto's, documenten, werkbestanden, agenda's en herinneringen. Daarom raad ik aan om voor Office weg te blijven bij Microsoft 365 en Google Docs als "standaard oplossing". Kies liever OnlyOffice als basis: gratis, robuust en zonder dat je documenten onderdeel worden van een commercieel ecosysteem. Alternatieven zijn LibreOffice of WPS Office.

Voor cloudopslag Proton Drive aanbevelen, de privacy-by-design is bedoeld om jouw bestanden echt van jou te laten blijven. Andere opties zijn CryptPad, Nextcloud of een privacyvriendelijke "workspace"-oplossing. Houd je mappenstructuur bewust simpel: Documenten, Foto's, Werk, Privé, Back-up. En voorkom de klassieke valkuil: "alles maar syncen" met Google Drive of OneDrive zonder te weten wat er precies staat, wie er bij kan, en wat er met je data gebeurt.

En dan back-ups: vertrouw niet alleen op syncen als back-up. Gebruik de 3-back-up aanpak: één online (bijv. Proton Drive), één versleutelde externe SSD in een afgesloten kast, en één goed verstopte versleutelde externe SSD op een andere plek. Gebruik de cloudkopie voor je dagelijks gebruik. En plan een vaste back-up momenten. Zo bouw je rust in: als er iets misgaat, ben jij niet je digitale leven kwijt.

## 7. E-mail

E-mail is een van de belangrijkste en tegelijk gevoelige digitale communicatiemiddelen. In je inbox zitten heel veel persoonlijke gesprekken, account-herstelmails, facturen en andere vertrouwelijke informatie. Veel mensen gebruiken nog steeds Gmail of Outlook. Die zijn "gratis", in ruil voor je privacy en vallen onder Amerikaanse wetgeving. Wie meer regie wil over zijn data, kan beter overstappen naar een privacyvriendelijke maildienst.

Veel betere keuzes zijn Proton Mail of Tuta Mail. Bij voorkeur de betaalde versie. Beide bieden sterke versleuteling en verdienen geen geld met advertenties of dataverkoop. De inhoud van je mails is voor hen niet leesbaar. Dat is een fundamenteel ander model dan bij Big Tech-maildiensten. Het gebruik is simpel: via web of app en het werkt verder net als gewone webmail, maar dan zonder tracking en profiling.

Het is praktisch is om meerdere e-mailadressen te gebruiken voor belangrijke zaken zoals bank, overheid en medische accounts, en een of meerdere aparte adressen voor webshops, registraties en nieuwsbrieven. Zo

voorkom je dat alles op één plek samenkomt en verklein je de impact bij datalekken of spam. Je kunt bij Proton ook aliassen gebruiken of een dienst zoals SimpleLogin inzetten voor wegwerp-adressen die mail tijdelijk forwarden.

Zet eventueel tijdens de overstap tijdelijk doorsturen aan vanaf je oude Gmail of Outlook, zodat je geen mails mist. Zet wat je wilt behouden over en delete de rest zo veel mogelijk. Vermijd een volgelopen oude mailbox zonder plan. Gebruik je Gmail of Outlook eventueel als "wegwerp"-adres. Dan stap je rustig en gecontroleerd en zonder stress over, terwijl je meteen een grote winst boekt in privacy en digitale zelfstandigheid.

## 8. Chat en videobellen

Dagelijks communiceren we via chat- en videodiensten zoals WhatsApp, Messenger, Zoom of Teams. Deze zijn erg handig, maar brengen structurele privacyrisico's met zich mee: vooral de metadata is extreem waardevol en wordt verzameld, geanalyseerd, gebruikt en doorverkocht. Daarom is het verstandig om deze communicatie te veranderen en liever niet alles via één platform te laten lopen. Signal is momenteel het meest gebruikte privacyvriendelijke alternatief voor WhatsApp. Het is gebruiksvriendelijk en sterk versleuteld, maar het is Amerikaans en gekoppeld aan je telefoonnummer en is daardoor een praktische tussenstap in de goede richting.

Al moeten we met z'n allen echt nog een stapje verder zetten, kies daarvoor het liefst voor SimpleX of Briar. Ook Session en ElementX zijn best goed. Ze hebben geen telefoonnummer nodig en minimaliseren metadata structureel. Briar heeft de hoogste beveiliging werkt alleen met tekst en is dus beperkt in functies en kan niet bellen of videobellen, SimpleX, Session en ElementX kunnen dat wel. Installeer het voor je meest naasten en wordt er goed in en overtuig andere vrienden, familie en collega's.

Voor videobellen is Peercalls heel eenvoudig en een uitstekende open-source keuze: direct, volledig anoniem en eenvoudig, direct in de browser en zonder account te gebruiken. Een andere Europese, maar commerciële oplossing is Whereby dit is een volledig anonieme open source oplossing maar is maar 30 minuten gratis maar heeft een betaalde versie voor grotere teams. Session is ook goed qua privacy maar Australisch. ElementX kan teamvideobellen maar is iets minder beveiligd dan de anderen.

Vermijd in ieder geval de alles-in-één-communicatie via WhatsApp, Meta-, Google- of Microsoft-platforms. Houd ze als "noodbrug" open maar stimuleer je belangrijkste contacten om over te stappen in ieder geval naar Signal, maar liever naar SimpleX, Briar en Peercalls. Deze bewuste keuzes geven privacy, vrijheid en regie over je data.

## 9. AI Tools

AI-tools worden razendsnel onderdeel van ons dagelijks leven: chatbots, vertalers, samenvatters en assistenten helpen ons sneller en slimmer werken. Maar veel van deze diensten draaien in de cloud bij grote (vaak Amerikaanse of Chinese) bedrijven. Wat je intypt, wordt opgeslagen, geanalyseerd en gebruikt voor training. Dat maakt ze krachtig en handig, maar ze hebben heel weinig respect voor je privacy.

Veel privacyvriendelijker zijn de Europese alternatieven. Le Chat van het Franse Mistral en Lumo van het Zwitserse Proton leggen veel nadruk op privacy en vallen onder strengere Europese/Zwitserse wetgeving. Ze zijn iets minder krachtig dan de BigTech varianten uit de VS en China, zoals ChatGPT, Claude, Gemini, Deepseek of Qwen, maar voor de gewone gebruiker goed genoeg.

De meest privacyvriendelijke optie is AI lokaal op je eigen computer draaien: dan verlaat je data je apparaat niet. Dat vraagt wel wat technische kennis en vaak een krachtige computer, dus is niet voor iedereen praktisch. Vermijd in ieder geval de BigTech AI-tools bij het delen van privacygevoelige data. Kies dan liever voor de Europese varianten, liefst met alias-email-account. Gebruik cloud-AI alleen voor niet-gevoelige zaken, en plak in online AI

nooit privégegevens, wachtwoorden, medische info, dagboekteksten of identificeerbare data. AI is een hulpmiddel, geen vertrouwenspersoon. Zo benut je de voordelen van AI, zonder je privacy op te geven.

## 10. Wachtwoordbeheer

Eén van de meest impactvolle stappen voor je digitale veiligheid is goed wachtwoordbeheer en het gebruik van 2FA (tweestapsverificatie). Veel mensen hergebruiken wachtwoorden of kiezen makkelijke varianten zoals "Welkom123", of slaan ze op in notities of losse tekstbestanden. Dat is vragen om problemen: als één dienst wordt gehackt, liggen vaak meteen meerdere accounts open. De oplossing is simpel en krachtig: gebruik overal unieke, lange en willekeurige wachtwoorden, en laat die beheren door een wachtwoordmanager.

Goede keuzes zijn Proton Pass, Psono, Bitdefender of een lokale oplossing zoals KeePassDX. Zo hoef je nog maar één sterk hoofdwachtwoord te onthouden, terwijl de manager voor elke dienst automatisch veilige wachtwoorden genereert en invult. Dit maakt je niet alleen veiliger, maar ook comfortabeler: geen gedoe meer met onthouden of resetten.

Zet waar mogelijk altijd 2FA aan. Aanbevolen zijn Aegis Authenticator of de 2FA-functies van Proton. Vermijd Google Authenticator en wees terughoudend met biometrie zoals vingerafdruk of gezichtsherkenning: dat is handig, maar geen geheim dat je kunt veranderen als het ooit uitlekt.

Het is verstandig om niet alles in één systeem te stoppen. Spreid je risico's over meerdere diensten en gebruik aliassen waar dat kan. Bewaar ook herstelcodes veilig in je wachtwoordmanager. Begin met je belangrijkste accounts zoals e-mail, cloud, sociale media en financiën, en werk stap voor stap verder. Met deze ene verandering maak je in één klap je digitale leven aanzienlijk veiliger én rustiger.

## 11. Encryptie

Encryptie is een belangrijk fundament van digitale privacy. Het klinkt technisch, maar in de praktijk is het vooral een eenvoudige en krachtige manier om jouw gegevens te beschermen tegen diefstal, misbruik en meekijken. De eerste en belangrijkste stap is volledige schijfencryptie op je laptop en telefoon.

Op moderne systemen is dit vaak al standaard aanwezig (zoals FileVault, BitLocker of LUKS op Linux, en device-encryptie op Android en iOS). Zonder de juiste pincode of het juiste wachtwoord is de data dan onleesbaar, zelfs als iemand de schijf uit je apparaat haalt. Dat maakt het verschil tussen "alles ligt op straat" en "je data zit in een kluis".

Daarnaast is het verstandig om gevoelige bestanden apart te versleutelen, zeker als je ze deelt of in de cloud opslaat. Denk aan tools zoals Cryptomator of VeraCrypt, of een met wachtwoord beveiligd archief.

Ook back-ups verdienen altijd encryptie, want ze bevatten letterlijk je hele digitale leven. Onversleutelde back-ups zijn een zwakke schakel. Belangrijk is ook dat je naast herstelcodes, back-upcodes ook je encryptie sleutels veilig bewaart, bijvoorbeeld in een goede wachtwoordmanager en eventueel ook offline.

In communicatie gebruik je vaak al encryptie zonder het te merken, bijvoorbeeld via Signal. Dat is goed, maar besef dat veel diensten jouw data zonder encryptie graag opslaan. Kies liever voor diensten die zelf niet bij jouw inhoud kunnen.

Encryptie werkt het best als je het meteen goed instelt en er een gewoonte van maakt. In dagelijks gebruik merk je er nauwelijks iets van, maar het beschermt je enorm. Het simpele principe is: versleutel alles wat belangrijk is, zowel in opslag als tijdens verzending. Dat is één van de meest effectieve manieren om jouw digitale autonomie te bewaren.

## 12. Andere BigTech apps vervangen

Met al deze stappen ben je veel losser van Big Tech gekomen. Toch gebruik je nog vele diensten die ongemerkt data verzamelen en je in algoritmes trekken. Dit laatste thema gaat over het opruimen van die rest. Je hoeft niet alles tegelijk te vervangen. Kies stap voor stap betere alternatieven. Verwijder voor elke nieuwe app die je installeert een paar oude Big Tech-apps. Zet tracking en locatie zoveel mogelijk uit en geef apps liever tijdelijk toestemming voor permissies. Wis regelmatig je geschiedenis en sluit apps na gebruik. Elke vervanging is een stap naar meer autonomie, rust en vrijheid. Laat technologie een hulpmiddel zijn in plaats van een datalek.

### Social media

Veel mensen zitten vast in Instagram, Facebook, TikTok en X (Twitter). Deze platforms zijn zeer verslavend en ontworpen om je aandacht zo lang mogelijk vast te houden, met eindeloze feeds, aanbevelingsalgoritmes en steeds extremere content. Je betaalt met je tijd, je aandacht en je data. Alternatieven zijn Pixelfed, Mastodon, Bluesky, RSS en PeerTube of podcasts. Zo kies jij wanneer en wat je kijkt, in plaats van andersom.

### Navigatie

Google Maps is handig, maar weet ook precies waar je bent, waar je heen gaat en wat je routine is. Uitstekende alternatieven zijn OpenStreetMap, HereWeGo en OsmAnd (offline maar betaald). En op Linux kun je GNOME Maps of Marble (KDE). Voor wandelen en natuur zijn Organic Maps, OpenTopoMap, Komoot en QGIS interessant.

### Agenda

Je agenda zegt veel over je leven: waar je bent, met wie je afspreekt, wat belangrijk voor je is. Kies in plaats van Google of Outlook Calendar voor Tuta Calendar of Proton Calendar. Verder zijn Nextcloud Calendar of Infomaniak alternatieven. Daarmee blijft jouw planning ook echt van jou.

### Notities en taken

In plaats van Google Keep, Microsoft To Do of andere cloudgebonden diensten. Goede alternatieven zijn Standard Notes, Joplin en CryptPad waarmee je online kunt synchroniseren. Of Obsidian lokaal op één device of betaald met online sync. Verder kunnen Proton Drive documenten of Todo.txt goed werken voor je notities en taken.

### Weer

Zelfs weer-apps verzamelen vaak locatiegegevens en gebruiksprofielen. Simpele en betrouwbare alternatieven zijn BlueMeteo, Buienradar of het KNMI. Die doen wat ze moeten doen: het weer laten zien, zonder onnodige tracking.

### Foto's

In plaats van automatische synchronisatie met Google Photos, One Drive of iCloud Photos, die je hele leven in beeld hebben en je data analyseren zijn er privacyvriendelijke alternatieven zijn Proton Drive Photos, Ente Photos en Immich of Nextcloud Photos als je zelf wilt hosten. Verder is je foto's regelmatig op een offline SSD back-up zetten een heel goed idee. Dan weet je zeker dat jouw foto's worden niet gebruikt om profielen te bouwen.

### Video en streaming

YouTube en Netflix zijn comfortabel, maar sterk gestuurd door algoritmes. In plaats van YouTube kun je FreeTube, PeerTube of Invidious gebruiken: je kijkt zonder tracking of account. Denk streaming aan NPO Start, Cinemember, Pathé thuis of Picl. Dan kijk je minder maar wel wat de moeite waard is. Overweeg bij social media om met een aliasaccount in te loggen en je geschiedenis te wissen en uit te zetten. Zoek dan zelf zonder algoritme wat je wil zien. Maak eventueel een document met je favoriete kanalen en onderwerpen. VLC is de meest privacy vriendelijke media speler voor Windows en Android. Celluloid is dat voor Linux.

### Muziek en podcasts

Spotify is handig, maar draait volledig om data en aanbevelingen. En de muzikanten verdienen erg weinig. Een mooi alternatief is Qobuz. En natuurlijk kan je ook lokaal je muziekbestanden (MP3, FLAC) afspelen met VLC of Celluloid mediaspeler. Bouw zelf je eigen muziekbibliotheek, in plaats van vertrouwen op het algoritme dat je smaak langzaam vervormt. AntennaPod is een privacyvriendelijke app voor gratis podcasts.

### Gamen

Schaken kan je beter niet via Chess.com doen maar via Lichess. En gamen gaat schijnbaar erg goed en privacyproof via Steam.

### Nieuws

Veel mensen krijgen nieuws via sociale media of gepersonaliseerde feeds. Dat zorgt voor polarisatie en bubbels. Een gezonde oplossing is een gerenomeerde nieuwzender of een RSS-reader, zoals FreshRSS, Feedly of Inoreader. Je kiest zelf welke bronnen je volgt. Geen eindeloos doorswipen in een denkrichting omdat het algoritme dat wil.

### Vertalen

In plaats van Google Translate kan je DeepL of LibreTranslate gebruiken voor je vertalingen. Zet geen gevoelige teksten in online vertalers, want je teksten worden opgeslagen en gebruikt voor training.

### Communities

Reddit is voor veel mensen dé plek voor informatie en discussies, maar het is ook een datamachine met tracking en commerciële belangen. Alternatieven zijn Lemmy, klassieke fora, nieuwsbrieven, en fysieke of lokale meetups.

### Reizen

Organisaties als Booking en AirBnB kan je vervangen door direct te boeken bij hotels/B&B's, dat is het meest privacyvriendelijk: geen groot platform ertussen, minder tracking, en je steunt de aanbieder direct. Je kan met een aliasaccount natuurlijk wel makkelijk zoeken op dergelijke sites.

## Bijlage 1 GrapheneOS installatie

Installatiestappen van GrapheneOS op een Pixel non-carrier-locked smartphone

GrapheneOS is een zeer privacygericht Android-alternatief. Het wordt vooralsnog alleen op Google Pixel-toestellen (Pixel 6 of nieuwer, niet carrier-locked) ondersteund. Kijk zeker ook op [grapheneos.org](https://grapheneos.org) en handig om AI je te laten helpen bij het installatieproces.

### Vereisten

- Pixel 6/7/8/9/10 (geen carrier-locked modellen).
- Computer met  $\geq 2$  GB RAM,  $\geq 32$  GB opslag.
- USB-kabel (geen hubs, directe aansluiting).
- Browser: Chromium/Chrome/Edge/Brave (geen incognito of VM, Brave Shields uit).

### Installatie in het kort

1. Update Pixel en zet OEM unlocking aan (Instellingen → Ontwikkelaarsopties).
2. Start in Fastboot Mode (Volume-omlaag + power bij opstarten).
3. Open GrapheneOS Webinstaller en verbind je Pixel.
4. Unlock bootloader (wist alles!).
5. Download & flash de nieuwste GrapheneOS-release.
6. Lock bootloader (wist opnieuw, *essentieel voor beveiliging*).
7. Start GrapheneOS en zet OEM unlocking uit (Instellingen → Ontwikkelaarsopties).
8. Verifieer met de *Verified Boot key hash* (gele waarschuwing bij opstarten) of Auditor.

### Belangrijk

- Bij een Carrier-locked smartphone werkt OEM unlocking werkt niet; dan lukt het niet om Graphene OS te installeren. Koop dus alleen een *unlocked* model.

Klaar! Installeer apps via F-Droid, Obtainium of Aurora Store (zonder Google-account). Gebruik Vanadium (beveiligde browser) en schakel Private DNS/VPN in voor extra privacy.

## Bijlage 2 Linux installatie

Installatiestappen waarmee je Linux Mint of Fedora op je Windows-computer zet:

Linux is open source, altijd gratis, veilig en zonder datastroom naar Big Tech. Je kunt vanaf een USB stick Linux eerst bekijken en proberen door op "Probeer" te klikken in het installatieproces.

Tip: Laat AI je helpen bij het installatieproces.

Dual-boot (Linux naast Windows):

1. Back-up belangrijke bestanden.
2. Download de ISO van Linux Mint of Fedora.
3. Maak een opstartbare USB met Rufus of BalenaEtcher.
4. Schakel Secure Boot en Fast Startup uit in Windows en BIOS/UEFI.
5. Verklein de Windows-partitie via Schijfbeheer en zorg voor voldoende vrije schijfruimte (50 GB vrije ruimte) naast de werkende Windows-installatie.
6. Start op vanaf de USB, kies "Installeer", en selecteer "Naast Windows installeren".
7. Maak partities (optioneel).
8. Installeer GRUB op de EFI-partitie (UEFI) of MBR (BIOS).
9. Start opnieuw op en kies bij het opstarten telkens voor Windows of Linux.

Volledige installatie (Windows verwijderen en door Linux vervangen):

1. Back-up alle gegevens – want alle data op de computer wordt gewist.
2. Maak een opstartbare USB met Rufus of BalenaEtcher en start hiervan op.
3. Schakel Secure Boot en Fast Startup uit in Windows en BIOS/UEFI.
4. Start op vanaf de USB, kies "Schijf wissen en Linux installeren".
5. Maak partities (optioneel).
6. Installeer GRUB op de hoofdschijf.
7. Start opnieuw op – Linux is nu het enige besturingssysteem.

Klaar! Geniet van Linux naast of in plaats van Windows!