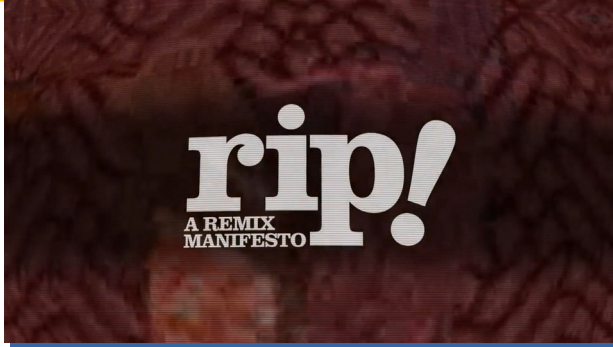


Stap Af van die Tech-Giganten



Huiswerk: 2 films van deze 6



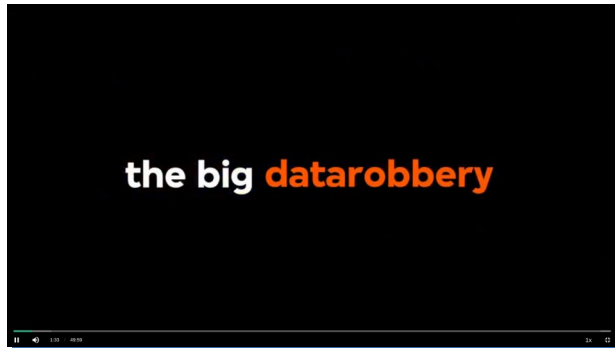
1. RIP A Remix Manifesto



2. You are being watched



3. Big tech is targeting you



4. The Big Datarobbery



5. Wie regeert de Smart City?



6. The Spyware on Your Phone that could End Democracy

RIP A Remix Manifesto

- Van wie is de sample?
- Hoe gaat youtube tegenwoordig om met Rights Management
- In hoeverre mag je samples van een ander hergebruiken
- Hoe werkt het met de rechten op software / code?

Rechten op software

Proprietary Software

- = eigendom
- Je 'koopt' het programma
- Slechts het recht om de binaire versie op 1 systeem

Free Software

- Je krijgt de code erbij
- Die je mag aanpassen
- Variatie in: of je de licentie vrij moet laten of naar "proprietary" mag
 - Fork-cultuur
 - 25 jaar Linux, 30 jaar GNU

The Big Datarobbery / Shoshana Zuboff

- Surveillance Capitalism
- Informatie die we zelf geven + bijvangst
- Info wordt verkocht en doorverkocht
- Data afval (hoe snel je typt, hoe je auto rijdt)
→ bruikbaar voor voorspellingen
- Data → om modellen te trainen
- Voorspelt: Personality, emoties, sexuele voorkeur, politieke richting, koopgedrag
- Verkoop: Moment van Top Kwetsbaarheid
- Gebruik van subliminals
- Vrijheid en democratie in gevaar



You are being watched

- NSA Might be spying on us
- Snitches and undercover cops in the digital real world
- Informanten nemen belangrijke plaatsen in organisatie
- Informant Brandon Darcy zet aan tot geweld (brandstichting)
- Informant levert bewijsstukken voor veroordeling

Smart Cities

- Regie hebben over processen in de stad
- Apparaten bedoeld om je / de massa te volgen
- Verstoep, verkocht, vermomd
- Niet alleen persoonsgegevens
- Utopie / Dystopie. Wie heeft dan die regie waarover?
- Stad komt in handen van bedrijven zonder democratisch toezicht
- Alleen maar afhankelijk worden van de vendors → zelf gegijzeld
- Elke afwijking is verdacht. Wantrouwen eerst.

Telsysteem bezoekersaantallen Maassluis

Dit is een **gearchiveerd** item.

Zoals bekend heeft de gemeente Maassluis onlangs een systeem aangeschaft om bezoekersaantallen in de stad te kunnen meten. Op 29 april 2021 heeft de Autoriteit Persoonsgegevens (AP) bekendgemaakt een boete aan de gemeente Enschede op te leggen voor wifitracking in de binnenstad. De AP is van mening dat de gemeente zonder grondslag indirecte persoonsgegevens heeft verwerkt van gebruikers van mobiele apparaten waarop de wifi stond ingeschakeld.

De uitspraak van de AP - waarin wordt gesteld dat mensen in Enschede werden 'gevolgd' op basis van wifi-signalen - is gebaseerd op zeer hypothetische situaties en aannames, niet op situaties die feitelijk hebben plaatsgevonden. Met de telmethode van Bureau RMC worden mensen geteld en niet gevolgd. Identificatie van individuen aan de hand van de verwerkte data uit de anonieme wifimeting is niet mogelijk.

Andere telmethode

Het is belangrijk om te vermelden dat de AP onderzoek in Enschede heeft gedaan naar een oude telmethode die sinds vorig jaar niet meer bestaat en dus niet vergelijkbaar is met het systeem dat we in Maassluis willen gaan gebruiken. De situatie waarin mensen theoretisch gezien kunnen worden 'gevolgd' door een MAC-adres te combineren met een direct persoonsgegeven, is onmogelijk gemaakt. Gegevens nu versleuteld worden en korter dan 24 uur worden opgeslagen. Het systeem voldoet de huidige methode aan de door de AP geschetste kaders.

Privacy

Op dit moment wordt door de gemeente uitgezocht in hoeverre het tellen van mensen via wifitracking zoals de gemeente Maassluis dat wil gaan doen, houdbaar is binnen de privacy wetgeving. Mocht de privacy in het geding zijn dan zal de gemeente naar alternatieve mogelijkheden kijken om bezoekersaantallen in kaart te brengen.

Deel via:



Contrast



Groter
AA

Lees voor


 Uw mening

Waarom afstappen van de tech-giganten?

- Wij zijn niet de klant. Wij zijn het product.
- Zij verdienen geld
- Wij krijgen de depressies
- Google, een front firma van de CIA / NSA
- Je gegevens worden verkocht
- De gegevens zijn waardevol want ze beïnvloeden al jouw aankopen
- Ze weten meer van je dan je denkt.
- Gegevens gaan een eigen leven leiden, geen verdediging mogelijk

Waarom Afstappen 2, 3 en 4

- Software en systemen:
 - “Heb” je dat programma dan echt?
 - Lawful Interception
 - Illegal Interception
- Protocollen op lager niveau als SMS bewust onveilig ontworpen
- Hardware Drivers op smartphone kunnen alles afluisteren (+- 10 per foon)
- Youtube: demonetization & deplatforming

Zelf de teugels in handen hebben!

- Opgroeien en opstaan
- Niet: *Oh God geef me een alternatief.*
- *Beter allemaal een ander alternatief dan weer allemaal hetzelfde paard*
- Zo geweldig als je het had bij hun wordt het gewoon niet
- 80-20 regel
- Focus op **wat wel lukt**
- **Begin makkelijk**
- Ik gebruik zelf dagelijks google services zoals webmaster tools (reCaptcha).
- Services waar geen alternatief voor is → *update: toch wel!*
 - Denk maar niet dat je ooit helemaal zonder komt
 - En dat hoeft ook niet
- Het gaat meer om de mindset dan om de realisatie

Waarom afstappen van de tech-giganten?

- Wij zijn niet de klant. Wij zijn het product.
- Zij verdienen geld
- Wij krijgen de depressies
- Google, een front firma van de CIA / NSA
- Je gegevens worden verkocht
- De gegevens zijn waardevol want ze beïnvloeden al jouw aankopen
- Ze weten meer van je dan je denkt.
- Gegevens gaan een eigen leven leiden, geen verdediging mogelijk

Wat gebruiken we

- **Beginners**

- Web Browser
- Browser extensies
- Search
- Mail
- Video
- Maps

- **Moeilijk**

- PC / Desktop
- Mobile

- **Lastig**

- Office / Bestanden
- Chat / Talk
- Things
- Social network

- **Had je al lang moeten doen**

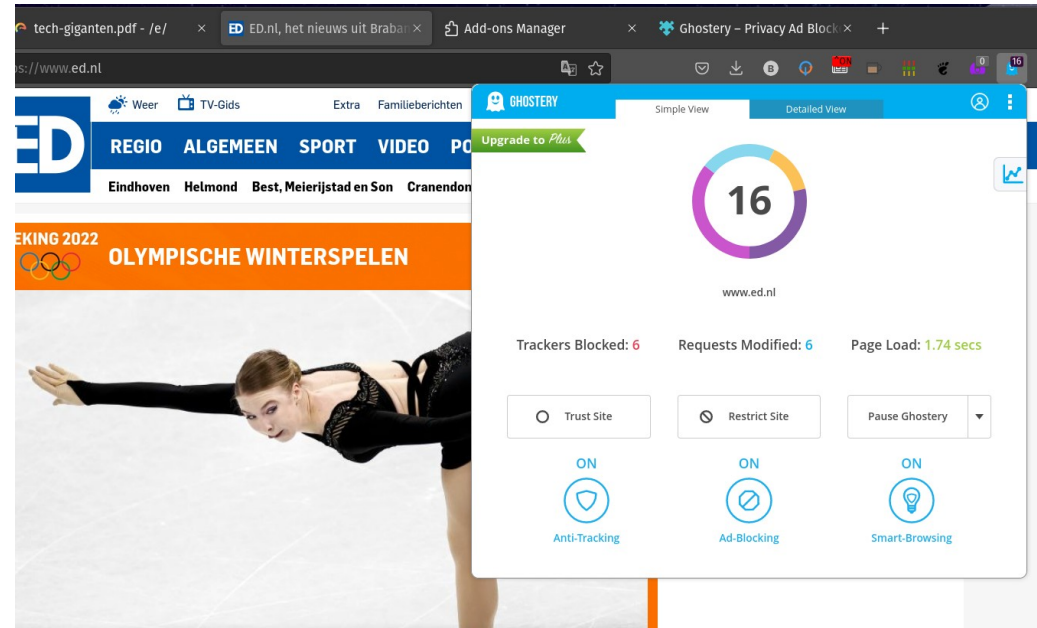
- Password Manager

Browser

- Is Google Chrome de voorpagina van de NSA?
- Safari (apple) status onbekend
 - Open Source kloon Chromium: Brave, Duckduckgo en alle anderen
 - Microsoft Edge, tsja.
- **Firefox** is het enige alternatief dat geen chromium-kloon is
- Opera is het kleine alternatief met de meeste jaren ervaring
- Tor browser voor Dark Web
- Torch browser voor streaming
- Epic met built-in privacy

Ghostery

- Niet de meest uitgebreide
- Niet de moeilijkste
- Aan- en uitzetten blijft een spel
- Mee leren werken





CLICKING ADS SO YOU DON'T HAVE TO.

As online advertising becomes ever more ubiquitous and unsanctioned, AdNauseam works to complete the cycle by automating ad clicks universally and blindly on behalf of its users. Built atop uBlock Origin, AdNauseam quietly clicks on every blocked ad, registering a visit on ad networks' databases. As the collected data gathered shows an omnivorous click-stream, user tracking, targeting and surveillance become futile. Read more about AdNauseam in this [paper](#).

Insta

- Klikkt op advertenties
- Die hij wel of niet toont
- Vervuult zo de databases van surveillance
- Banned by google
- Recommended by Firefox
- Uitzetten, als de site niet werkt

Search

- Standaard zoekmachine staat al gauw op google.com
- Pas de standaard zoekmachine aan in de browser
- Installeer browser extensie voor de zoekmachine
- Demo Video. <https://youtu.be/7JZdtifXt1U>
- ~~Startpage.com~~
- Duckduckgo.com
- Ecosia.com
- **Swisscows.com**
- Searchencrypt.com
- En Vele Anderen

Mail. En je zit weer jaren vast

- Gmail.com lekker makkelijk en gratis.
- Hotmail de vorige bekende gratis dienst
 - Met een eigen website → je mail is al betaald
- Je hebt meestal mail bij je ISP service “@caiway.nl”

Kijk eens bij

- Mailfence
- Tutanota
- **Protonmail.com**
- Countermail
- Runbox
- Nextcloud (!)

E-mail Programma op pc

- Een pc- of mobile app die algemeen bruikbaar is
- Met de hand instellen of automatisch
- De webmail versie maar hoe handig is dat?
- **Thunderbird**
- Claws Mail
- Sylpheed
- Mailspring

Video

- Youtube is net zo'n propagandamiddel als de televisie zelf.
- Toxic algoritme dat verslavend werkt als suiker
- Een self-hosted videoplatform is een optie met:
- Peertube
- Mediagoblin
- Rumble
- Bitchute
- D.tube
- Brighteon
- Bittube
- Odysee = LBRY
- **LBRY**



LBRY



Search



545.83



Home



Following



Your Tags



Discover



Library



Lists

Your Tags

Trending

New

Top



Manage



Movie: The Visitor from Planet Omicron



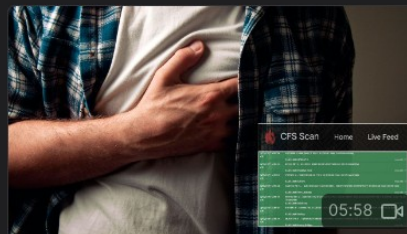
@christoph.egger138
6 days ago



Blender 3.0 - Every New Feature in 6 minutes



@Blender
2 days ago



Tracking "Chest Pain" in South Australia



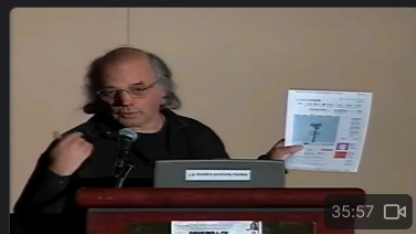
@JWild
3 days ago



Refusing To Use Programs Written In Python



@DistroTube
22 hours ago



The COVID Vaccine War - the final takeover of the biological compute...



@HumanitysVault
4 days ago



Liberty Live Stream III - Episode 63



@RichardHarrisCoaching
1 day ago



Poland House Of Representatives' Investigation Committee...



@HumanitysVault
3 days ago



What's Going On? Vol. 2



@JWild
6 days ago

OpenStreetMap

https://www.openstreetmap.org/#map=11/51.9464/4.2926

OpenStreetMap

Edit

History

Export

GPS Traces User Diaries Copyright Help About

Log In

Sign Up

Search

Where is this?

Go



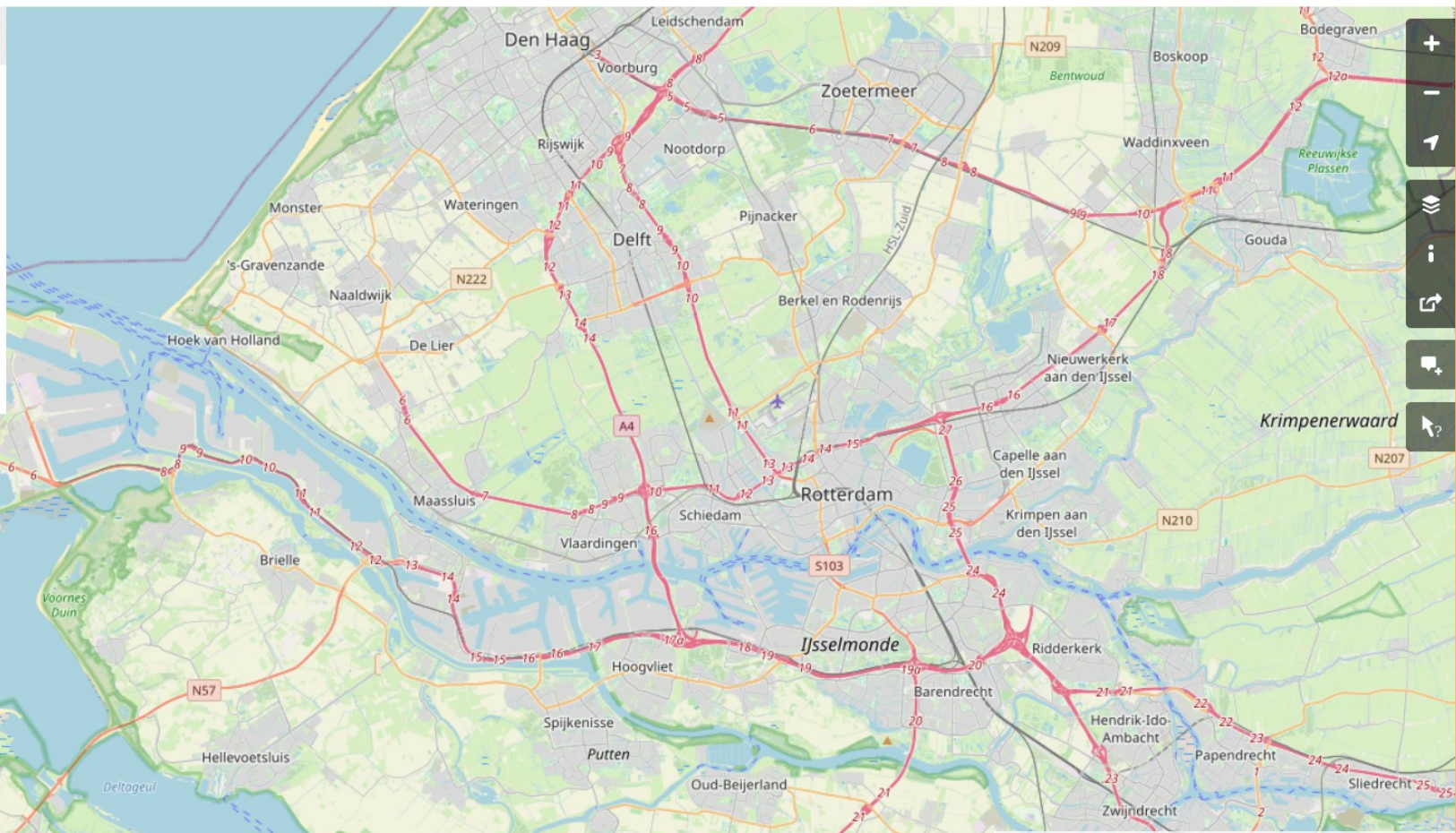
Welcome to OpenStreetMap!

OpenStreetMap is a map of the world, created by people like you and free to use under an open license.

Hosting is supported by [UCL](#), [Fastly](#), [Bytemark Hosting](#), and other [partners](#).

Learn More

Start Mapping



Wat gebruiken we: Lastig

- **Lastig**
- Office / Bestanden
- Chat / Talk
- Things
- Social network

Office / google drive

- LibreOffice is prima
- Cloud optie mist

- Nextcloud hub
- Als een service huren
- 1 NL aanbieder
- **thegood.cloud**



Chat / talk

- **Telegram**
- Code is GPL
Licentie :-)
- Wat gaat er naar de server?
- **Signal** – net ietsje beter maar is dat nu ‘t verschil dan?
- matrix.org heeft een veilige oplossing die net te lastig is voor Henk & Ingrid
- **BigBlueButton** is een uitstekende video call oplossing

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS



(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• Message Content: Limited • Subpoena: can render basic subscriber information • 18 U.S.C. §2703(d): can render 25 days of iMessage lookups to and from a target number¹ • Pen Register: no capability² • Search Warrant: can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return³; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud⁴	• Message Content: Limited⁴ • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage ⁴Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• No Message Content • Date and time a user registered • Last date of a user's connectivity to the service	• No Message Content • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities	• No Message Content • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• No Message Content • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number¹	• No Message Content • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• Message Content: Limited² • Subpoena: can render basic subscriber records • Court Orders: Subpoena return as well as information like blocked users • Search Warrant: Provides address book contacts and WhatsApp users who have the target in their address book contacts • Pen Register: Sent every 15 minutes, provides source and destination for each message ²If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• No Message Content • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number



SUBSCRIBER DATA



MESSAGE SENDER/RECEIVER DATA



DEVICE BACKUP



IP ADDRESS



ENCRYPTION KEY(S)



DATE/TIME INFORMATION



REGISTRATION TIME DATA



USER'S CONTACTS

<https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html>

Exclusive

Israel police uses NSO's Pegasus to spy on citizens

Mayors, leaders of political protests against former Prime Minister Benjamin Netanyahu, and former governmental employees, were among those tracked by police without a search or bugging warrant authorizing the surveillance

Tomer Ganon 07:03 18.01.22

TAGS: [NSO](#) [Pegasus](#) [Police](#) [Surveillance](#)

Israel police uses NSO's Pegasus spyware to remotely hack phones of Israeli citizens, control them and extract information from them, Calcalist has revealed. Among those who had their phones broken into by police are mayors, leaders of political protests against former Prime Minister Benjamin Netanyahu, former governmental employees, and a person close to a senior politician. Calcalist learned that the hacking wasn't done under court supervision, and police didn't request a search or bugging warrant to conduct the surveillance. There is also no supervision on the data being collected, the way police use it, and how it distributes it to other investigative agencies, like

Recently Read



"If Wiz is worth \$6 billion, Palo Alto is worth more than a



SentinelOne's \$2.5 billion takeover of Orca Security falls



Things

- GPS
- Google Nest
- Amazon Ring, Echo, Alexia
- Smart devices
- Body scanners
- Kinderspeelgoed
- Sex toys
- Smart meter (gas water licht)
- Parkeer app

- Vertrouw je deze knakkers?
- Met je dagelijkse data?
- Ik heb 100.000 scrobbles op last.fm?
- Mijn strava sport-prestaties ?
-
- Opletten en blijven opletten
- **Virtuele identiteiten / nicknames / email adressen / tel.nrs. apart houden**

Social Networks

- Er is niks zo vol gebruikers en gemak als de echte facebook en instagram, twitter
- Kom je erin, staat er dus niks op.
- “Extreem-rechts” is natuurlijk media-onzin
- Parler.com
- Minds
- **Mastodon**
- Enige met een verhaal anders dan “de kloon van”
- Charles Eisenstein’s
- **Naas Community**

Wat gebruiken we: Moeilijk

- **Moeilijk**
- PC / Desktop
- Mobile

PC / Desktop

- Windows 10: Is dat de Master of Spyware?
- Je moet inloggen met je Microsoft Account op je “eigen” computer.
- Power users “breken dan in” op hun eigen computer
- Microsoft – De eeuwige vijand van de vrije software tot 2015
- Sinds 2015 is Microsoft de grootste bijdrager aan de Linux Kernel. Zwart-wit?
- Advies: niet-kritische pc-systemen ombouwen tot Linux.
- Rare hardware en drivers eerst testen / checken
- Bij elke aanschaf (videocard, wifi, USB gadget) op blijven letten. Drivers suck.

Apple macOS

- Apple luistert je pc wat minder erg af. Maar Siri staat aan.
- Maar beperkt je vrijheden in de keuze van hetgeen je aankoppelt. Voor alles een eigen apple stekker of app.
- MacOS is familie van Unix, net als Linux
- Dus vrije software is eenvoudig toe te voegen en vrijwel altijd beschikbaar en betrouwbaar
- Advies: kat uit de boom kijken en bij volgende vervanging afvragen of je uit het Apple-ecosysteem stapt.

Linux

- 25 jaar free software
- 200+ varianten
- Server, cloud, things landschap is al grotendeels linux
- Eigenlijk alleen de Personal Computer nog niet.
- Je moet iemand hebben die je op weg helpt
- Als het loopt kan iedereen het bedienen
- Mijn top-5

Linux distributie top-5

- 1 Pop!_OS
- 2 Linux Mint, Cinnamon
- 3 Fedora
- 4 Ubuntu
- 5 Manjaro

Full-disk installeren of dual-boot maken

- Dual-boot = als je opstart kun je nog kiezen voor die ander
- Download de ISO en brand de USB Stick met Balena Etcher
- Al je bestanden backuppen.
- Opstarten met USB erin. Check de boot-opties (F1, F10)
- Volg de installer
- Leerlingen 1-mavo over Linux Mint 2016:
- *Meneer dit is makkelijker dan Windows Installeren*

Mobile Opties

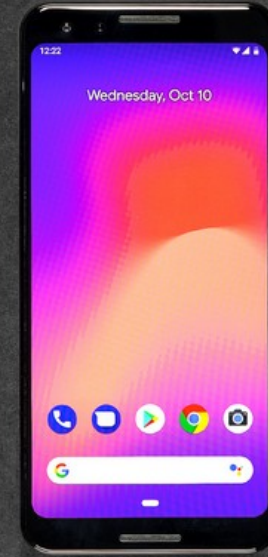
- Apple iPhone forget it
- Android forks: LineageOS, / e / , grapheneOS
- Linux: Ubuntu Touch, PostmarketOS, LuneOS, sailfish
- Zelf 'flashen' is niet zo makkelijk
- Een voorgeïnstalleerde kopen is makkelijker
- Er zijn ook fabrikanten met eigen modellen en een eigen systeem erop

Zelf leuk doen met smartphones

- Kies uit 1 van de systemen, bijv LineageOS
- Gaat je (extra) toestel het doen met dit systeem? bijv. Fairphone 3?
- Volg de installatie instructies voor deze combi
- Dit is echt werk voor een expert die een uitdaging zoekt.
- Vervolg meeting!

Rob Braxman

- Onafhankelijk vlogger met kleine shop in privacy tech
- Volop modellen ungoogled smartphones voor een nette prijs
- [Brax.me](https://brax.me)
- Rob Braxman [op LBRY](#)



Google Pixel 3 (De-Googled) Lineage 18.1

Google Pixel 3 (Used - Very Good Condition)
installed with Lineage 18.1 with No-GAPPS.

This phone is waterproof and has an
outstanding camera. This is Grade A quality.

Compatible with all carriers.

Comes with cable and power supply.... [More...](#)

399.00 US Dollar

[Create account on Brax.Me to use the
Store](#)

E foundation

Workspaces Applications

Broken clouds, 4.5 °C dec 5 22:13

en 100 %

OpenStre Oude wijs ontologis #124 - Het RIP A Rem The Age » You Are B ungoogle 12 Custom Murena x

← → ↺ https://esolutions.shop/shop/murena-fairphone-3-plus-fr/?wcpbc-m ☆

Select your language and country to shop online → English Netherlands

 **esolutions.shop**
your one stop shop for privacy!

SMARTPHONES ACCESSORIES SUPPORT MY ACCOUNT 



Murena Fairphone 3+

The deGoogled Murena Fairphone 3+ is the next evolution in privacy conscious and sustainable phone. It features 2 new camera modules with 48MP camera and 16MP selfie camera for higher quality pictures and videos and it is made of 40% recycled plastics, the most post-consumer recycled plastic of any Fairphone.

Like the Murena Fairphone 3, it features a removable 3000 mAh rechargeable battery and with its replaceable modules, you can repair it your self with a single screwdriver.

If you love to take beautiful pictures and care about fairer technology, this is your perfect companion.

473,81€

Available on backorder

- 1 +

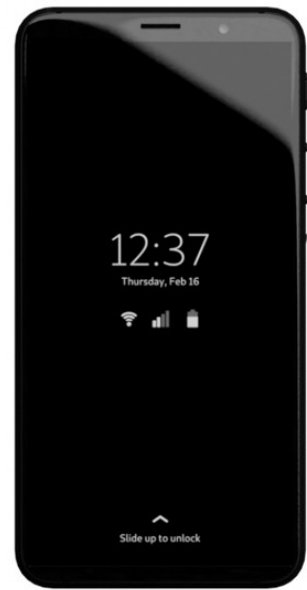
Pre-Order Now

0



- [Back to main website](#)
- [All products](#)
- [My Account](#)
- [Support](#)
- [Cart](#)

Home / Phones / Librem 5

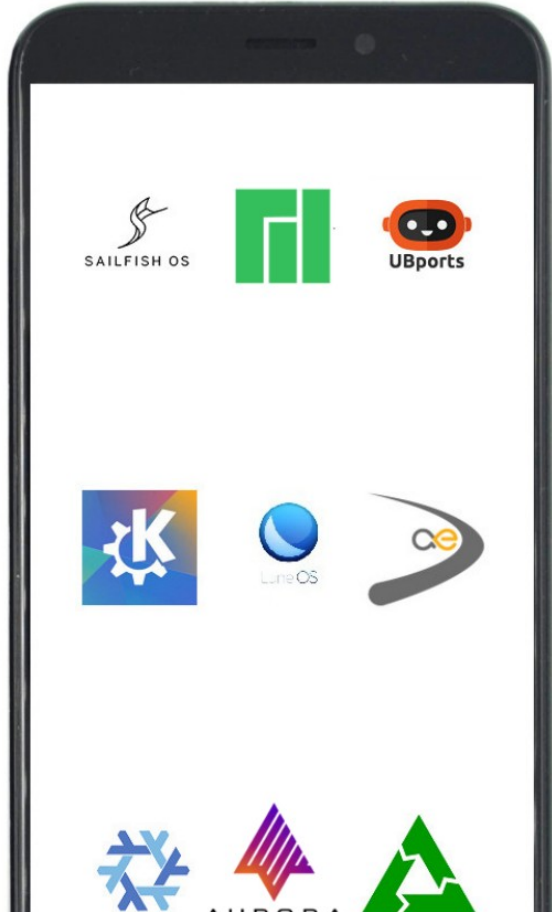


Librem 5

From: \$1,199.00

Librem 5, the phone that focuses on security by design and privacy protection by default. Outfitted with hardware kill switches and specially designed hardware, you are in control of the flow of information. [Learn more about the Librem 5...](#)

Backorder shipping resumes October 2021. Lead time for new orders: 52 weeks.
[A post about the electronics supply chain from Purism CEO Todd Weaver](#)



PinePhone

Quad-Core Allwinner A64 @ 1.152 GHz

Up to 3GB LPDDR3 RAM

Quectel EG25-G with worldwide bands

Bootable microSD and 16GB/32GB eMMC

Kill switches for LTE, Cameras, Wifi/BT, and Microphones

Six pogo pins allowing for custom hardware extensions

Go to Store 

Wat gebruiken we: Had je al lang moeten doen

- Had je al lang moeten doen
- Password Manager

Had je al lang moeten doen: password manager

- Telkens hetzelfde wachtwoord. Madness.
- Wachtwoorden in mailbox of in een word document. Op je Google Drive.....
- WW-manager van Firefox, Chrome al beter dan plaintext
- Voor paypal, bank, pincode, DigiD en zakelijk spul neem een echte
- Als je nu ergens een tientje aan uitgeeft dan is dit de plek
- Eerste start is demotiverend
- Na 1/2 jaar gebruik je m pas echt goed
- Uiteindelijk ben je er dan wel blij mee.
- Bitwarden
- Enpass
- 1password
- Keepass
- Nog veel meer opties.
- Check je behoefte voor mobile etc
- Sync de versleutelde kluis op je systeem en/of kopie in de cloud.... Daar gaan we weer!
- Check “de source”...

Conclusie

- Software en hardware zijn er klaar voor
- Het **waarom** is nu ook duidelijk
- Stap voor stap, geen haast, geen gekke dingen doen
- Zorg dat je zelf de zaak in eigen hand neemt.
- Ik kan geen 700 mensen + bedrijven + smartphones redden, dat moet je zelf doen.
- Internet helpt je!

Oproep

- Geef deze presentatie ook een keer in jouw kring
- Zakelijk vervolg?
- Smartphone install party?

Klaar?

- Ah nog 1 dingetje vragen?
- Je nieuwe auto met 'smart mobility'?

Barry Voeten

- Barry @ voeten . com
- 06-23056217
- Signal / Telegram /
Phone / SMS
- Maassluis
- Docent Informatica
- Groei of Evenwicht
- Kleureneconomie
- Aura van Bomen
- Paardendrummer