Data
Privacy

Privacy vs Security vs Anonymity

- Privacy – Controlling who has access to your data
- Security – How is data stored and how it’s secured from unauthorized access
- Anonymity – Hiding your identity, being unidentifiable

Privacy vs Security vs Anonymity - Examples

- Tor – Anonymity – you can change the circuit and appear as someone else
- Google security – good; data encrypted on servers from unauthorized access, e.g. hackers
- Google privacy – terrible; scans all your emails and is in every corner of your life to give you ads

Privacy

- “I have nothing to hide” is an invalid argument, though frequent when asking about online privacy
- Would you give your home address to a stranger
- Why does a stranger – Big Tech employee – have access
- By protecting your privacy, you’re controlling access to/protecting your (not only – also your close/loved ones) data

Privacy – examples of data abuse

- Tesla employees watched people even during intimate moments
- Google locked dad’s account after sending an image of his naked toddler to a doctor after flagging it as CSAM (Child Sexual Abuse Material)
- Meta spying on Android users using localhost

Ok, that sucks, but why should we bother

- You can be manipulated using ads
- There’s a billion dollar industry to collect and sell as much data about you as possible
- An AI model can, given your internet activity, determine you’re a threat to, e.g. a country you’re entering

What can we do about it

- Use F(L)OSS – Free (Libre) and Open Source Software
- Harden privacy wherever needed/possible
  - GitHub Privacy-Settings
  - Techlore Resources, PrivacyGuides.org
  - Alternativeto.net with Open Source filter
- Spread the word
- Support FOSS instead of Big Tech

What can we do about it – FOSS – Frontends

- Youtube – Invidious (web), NewPipe (Android)
- Twitter/X – Nitter (web)
- GitHub – GotHub (web), Forgejo (selfhost)
- AI
  - API + LiteLLM + OpenWebui
  - Duck.ai
  - Proton Lumo
  - Venice.ai – their uncensored model is available on HF

What can we do about it – FOSS – OS

- Linux
  - Beginners
    - Linux Mint
    - Fedora
  - Intermediate
    - Tinker with your current distro
  - Advanced
    - Arch Linux

What can we do about it – OS - Android

- Google Pixels – paradox – you win
  - GrapheneOS – talked about more later
- Others, depending on model
  - /e/OS
  - CalyxOS (paused), LineageOS
- Otherwise, GitHub Privacy-Settings

What can we do about it – OS – Android – GrapheneOS

- Features
  - Network and Sensor permission
  - USB C/pogo pins control
  - Storage/Contact Scopes
  - Wi-Fi privacy
  - Auto Reboot
  - Improved User Profiles – more, end session, disable app

What can we do about it – FOSS – App Stores

- Android
  - F-Droid (only FOSS apps)
  - Aurora Store (a privacy-respecting anonymous frontend for Google Play Store)
  - Obtainium/Sideloading (*Google wants to limit/remove)
  - Exodus and Plexus - analysis (permissions/trackers/loggers) and DeGoogled/MicroG compatibility
- iPhones – only EU
  - AltStore

What can we do about it – FOSS – Browser

- Normal usage
  - Chromium-based
    - Brave
    - Chromium
  - Firefox-based
    - Librewolf (Security-, privacy- and user-freedom-focused)
    - Hardened Firefox (Librewolf already does it)
    - Mullvad Browser/Tor Browser – Private Window only

What can we do about it – FOSS – Search Engine

- Brave Search – 100% independent index
- Duckduckgo – majority Bing + independent index + specialized search engines for “restaurants, lyrics, sports scores, etc.”
- StartPage – Bing + Google proxy
- Mullvad Leta – Google + Brave proxy
- Searxng – Selfhostable metasearch engine

What can we do about it – FOSS – VPN

- Why?
  - IP Address Hiding: Your VPN gives you a new public IP address, masking your real one.
  - Network Encryption: All internet traffic is encrypted ensuring secure communication e.g. on public Wi-Fi
  - DNS Query Protection: VPNs route DNS queries through their servers, preventing ISPs from logging which websites you visit.

What can we do about it – FOSS – VPN

- Proton VPN – free tier + Proton ecosystem
- Mullvad VPN/IVPN – only paid tier; fully anonymous account (no email, etc), Monero payments
- No-logs
- DNS servers
- Killswitch
- Tracker and ads protection

What can we do about it – FOSS – Email

- Proton Mail
  - PGP (subject lines not E2EE)
  - Unlimited aliases using Proton Pass/SimpleLogin
    - Ability to immediately disable/remove
  - Additional addresses
- Tuta Mail
  - Same encryption algorithms, but full E2EE
    - Aliases, but max of 15 (behave like additional addresses)

What can we do about it – FOSS – Password Managers

- Proton Pass
- Bitwarden
- KeePass
  - KeePass – requires addition work, below configured clients
  - KeePassDX client (Android – Fdroid)
  - KeePassXC client (Windows, MacOS, Linux)

What can we do about it – FOSS – Cloud Storage

- Proton Drive
- Tuta Drive (TBA)
- Cryptomator – use with Google Drive, etc.
  - Encrypts data and metadata before sending (you can verify by looking in your drive)

What can we do about it – FOSS – Messengers

- SimpleX – highest anonymity – no ID; no email or even random ID
- Signal – Most widely known and used
  - Molly (Android) – More secure Signal fork
- Matrix – decentralized communication (comp. email)

Thank you for Your Attention