Open Operating Systems

Open vs Closed Software — Privacy, Control, and the Linux Alternative

Łukasz Gołek

WIMiC AGH

Privacy | Open Source | Linux | Security | Encryption

What Is Open Source Software?

SECTION 1 · FUNDAMENTALS

Human-readable (source code)

```
#include <iostream>

int main() {
    std::cout << "Hello, World!"
              << std::endl;
    return 0;
}
```

Computer-readable (binary only)

```
00000000  7f 45 4c 46 02 01 01 00
          00 00 00 00 00 00 00 00
00000010  02 00 3e 00 01 00 00 00
          04 00 28 00 00 00 00 00
00000020  00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00
...
```

✓ Thousands of developers worldwide can inspect the source — bugs and malicious code get found. Open = transparent = secure.

What Is Closed Software?

SECTION 1 · FUNDAMENTALS

With closed software, you only receive the binary:

```
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  02 00 3e 00 01 00 00 00  04 00 28 00 00 00 00 00  |..>.......(.....|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
...
```

No source code

You cannot verify what the software is doing — ever.

No independent audit

Only the vendor can check for bugs or backdoors.

Used against you

Corporations exploit this to harvest your data and limit your freedom.

SECTION 2

Consequences of Closed Software

Control · Tracking · Costs · Security

Why Closed Software Hurts Users (1-4)

SECTION 2 · CONSEQUENCES

1

Lack of Control Over the Software

You cannot verify how the software works. Bugs cannot be fixed independently, nor can you customise it to meet your needs.

2

Dependence on the Vendor

The vendor controls the roadmap, updates, and end-of-life. If support ends, you are forced to pay for upgrades.

3

Risk of Tracking and Undesired Features

Closed software frequently collects user data without transparency, and may include DRM mechanisms that restrict your use of purchased products.

4

Higher Costs

Licenses, subscriptions, and vendor lock-in make switching expensive. You pay forever for the privilege of having no control.

Why Closed Software Hurts Users (5-8)

SECTION 2 · CONSEQUENCES

5

No Independent Security Audits

Vulnerabilities cannot be found by outside experts. If the vendor doesn't patch, users stay exposed indefinitely.

6

Limited Repair and Customisation

You depend entirely on vendor support. You cannot add features, fix issues, or modify the software even when you desperately need to.

7

Risk of Losing Access to Personal Data

Proprietary formats trap your data. Vendors can block access to your own files — as Adobe has done in sanctioned countries.

8

Compatibility Issues

Vendors deliberately break interoperability with competitors and force upgrades by breaking older version compatibility.

Real-World Examples

SECTION 2 · COMPARISON TABLE

Issue	Microsoft	Google	Apple	Other
Lack of Control	Windows 11 forces automatic updates, sometimes breaking older hardware/software.	Google restricts Android sideloading and adds security warnings.	iOS only allows App Store installs — jailbreak required for anything else.	Meta changes algorithms without notice, affecting content visibility.
Vendor Dependence	Microsoft discontinued Windows 7 and old Office, forcing paid upgrades.	Google stops updating Pixel phones after a few years.	Apple stops macOS support for older Macs, making hardware obsolete.	Adobe moved to subscription-only, eliminating perpetual licences.

Real-World Examples

SECTION 2 · COMPARISON TABLE

Issue	Microsoft	Google	Apple	Other
Risk of Tracking	Windows 10/11 collect extensive telemetry even if users try to disable it.	Google tracks location even with location services turned off.	Apple collects analytics from iPhones even if users opt out (per lawsuits).	Meta tracks users across the web using invisible trackers, even when logged out.
Higher Costs	Microsoft 365 replaces one-time purchase with a subscription model.	Google takes 30% from Play Store and enforces its in-app payment system.	Apple takes 15–30% commission and forces use of its payment system.	Adobe Creative Cloud cuts access to your work if you stop paying monthly.

Real-World Examples

SECTION 2 · COMPARISON TABLE

Issue	Microsoft	Google	Apple	Other
No Security Audits	Windows is closed-source — experts cannot fully audit it for vulnerabilities.	Google Play Services is closed-source, preventing full security audit of Android.	iOS is entirely closed-source — independent verification is impossible.	WhatsApp's encryption is controlled by Meta — users must trust without evidence.
Limited Repair & Customisation	Microsoft locks down Surface devices, making self-repair very difficult.	Google makes bootloader unlocking difficult, voiding warranties if modified.	Apple's 'Right to Repair' restrictions disable features if unofficial parts are used.	John Deere prevents farmers from repairing their own tractors via DRM.

Real-World Examples

SECTION 2 · COMPARISON TABLE

Issue	Microsoft	Google	Apple	Other
Losing Personal Data	Microsoft OneDrive users locked out due to policy violations or account issues.	Google can suspend accounts without warning — cutting access to Gmail, Drive, Photos.	Apple has locked iCloud accounts for policy violations, sometimes without explanation.	Adobe banned users in sanctioned countries from accessing purchased software.
Compatibility Issues	Microsoft makes old Office incompatible with newer Windows to push upgrades.	Google's proprietary services work poorly on non-Chrome browsers.	Apple deliberately prevents iMessage from working on Android.	Tesla uses proprietary software, making third-party repairs very difficult.

Google's Remote Control Over Your Android

SECTION 2 • CASE STUDY

Google Play Services (closed-source)

Has extensive device permissions. Can silently install, remove, or update apps — even without user consent.

Silent App Installation — Real Examples

2020: 'COVID-19 Exposure Notification' app pushed to millions without consent.
2019: Hidden security update pushed to Play Services — no opt-out possible.

Remote App Removal

Google can remotely uninstall any app flagged as malicious or policy-violating — VPNs, emulators, and other unapproved tools have been removed.

Android Enterprise / Device Owner Mode

In managed mode (typical on work phones), Google can push apps, change settings, and lock users out entirely.

Firmware Backdoors & Hidden APIs

SECTION 2 · CASE STUDY

Manufacturer Backdoors (especially Chinese brands)

Some Android devices from Chinese manufacturers may have hidden mechanisms allowing the manufacturer or carrier to remotely modify the system — outside the OS, at firmware level.

Can Google Execute Code Like the NSA?

Google does not have root access, but Play Services and hidden APIs allow significant control. With pre-installed Google apps (virtually all standard Android phones) Google can technically execute code, push updates, and install/remove apps — often without explicit user consent.

⚠ The line between 'remote management for security' and 'backdoor' is a matter of consent and transparency — both of which are missing here.

Microsoft & Apple Remote Control

SECTION 2 · CASE STUDY

Windows Update

Can push updates that modify system behaviour, install new features, or remove programs. Windows 10/11 send telemetry to Microsoft without clear user consent.

Remote Control via Intune

For enterprise devices, Microsoft can manage, push updates, and install apps remotely — including potential code modifications.

UWP Platform Lock

Microsoft enforces a store model where apps must pass through its review process, limiting users from running arbitrary code.

App Store Control

Apple requires all iOS apps to be downloaded via the App Store — the only gateway to the entire platform.

Remote OS Updates

Although iOS is closed-source, Apple can update it remotely through the App Store or system update mechanism.

Apple Device Management (ADM)

In enterprise settings, Apple can push updates, remove apps, and manage settings. Technically, Apple can execute code remotely on any iPhone.

Microsoft

Apple

Why Does This Matter — and What Can You Do?

While remote management is usually framed as 'security', it raises a fundamental question about who controls your device — and your data.

Custom ROMs

GrapheneOS or LineageOS — Android without Google Play Services. Full AOSP, no surveillance layer.

Block Google Services

Restrict internet access for Google Play Services and limit permissions via Android settings.

Alternative App Stores

F-Droid offers free/open-source apps only. No tracking, no proprietary dependencies, no Google.

Jailbreak (Apple)

Removes Apple's software lock. Introduces other risks — use with caution and solid security hygiene.

SECTION 3

Disk Encryption & Corporate Keys

Who really holds the keys to your data?

Real-life Consequence: Who Holds Your Key?

SECTION 3 · ENCRYPTION

Microsoft (by default) keeps a backup of your disk encryption key on its own servers.

What this means for you

Even with BitLocker enabled, Microsoft can — and will — hand your decryption key to authorities upon request.

Your encrypted disk is not private. It is privately encrypted with a key you do not fully control.

Disk encryption has no real purpose if a corporation holds the decryption key. True privacy requires you to hold the only copy of your key.

Corporate Disk Encryption Keys — What It Means

SECTION 3 · ENCRYPTION

All three companies claim zero-knowledge principles. All three retain the ability to decrypt your data under 'certain conditions'.

Apple

Claims 'zero-knowledge'. In practice: may provide data access at law enforcement request. Has access to encrypted iCloud backups.

Google

Stores encryption keys for Google Drive and all cloud services. Can decrypt and provide access per its privacy policy or during investigations.

Microsoft

Windows 10/11 and OneDrive encryption — Microsoft holds keys. Can access user data if required by law or for other stated reasons.

Authorities can obtain your data via court order — without your knowledge.

A company data breach exposes ALL user encryption keys simultaneously.

The company itself may misuse the keys — you have no way to verify they don't.

Further Risks of Corporate Key Custody

SECTION 3 · ENCRYPTION

Authority Access According to Law

Court orders or law enforcement requests can compel disclosure of your encrypted data. Apple has been forced to cooperate in past terrorism investigations. Google and Microsoft receive thousands of requests per year.

Risk of Data Loss via Company Hack

If the company's key management infrastructure is breached, all user data encrypted with those keys becomes accessible to attackers at once.

Potential Misuse by the Company

Users have no independent way to verify that keys are used only as stated. Internal actors, rogue employees, or undisclosed policy changes could compromise data.

Lack of Trust in Cloud Encryption

'Encrypted cloud storage' marketed by these companies is security theatre — they hold the keys and can access everything. Real privacy requires client-side encryption where only you hold the key.

What Actually Works: Real Encryption

Corporate encryption is theatre

If you are not worried about physical theft of your device, disk encryption by a corporation provides no real protection — data theft occurs at the OS level, where they already have access.

BIOS password > BitLocker

Securing your BIOS with a password is far more important than relying on OS-level encryption like BitLocker, which Microsoft controls.

LUKS — encryption that actually works

Linux Unified Key Setup (LUKS) is a free, open-source, audited encryption standard where ONLY YOU hold the decryption key. No company, no government, no cloud. Your key, your data.

SECTION 4

Why Use Open Source at All?

The political and practical case for Linux

The Stakes Have Never Been Higher

SECTION 4 · WHY OPEN SOURCE

The owners of the largest data-collecting corporations, following the recent elections in the USA — the global military and economic superpower — have become lawmakers.

For users of modern communication technology, nothing worse could have happened.

What this concentration means

The same companies that collect your data now also write the laws that govern data collection. The conflict of interest is total. There is no regulatory check.

Using their software is no longer simply a privacy risk — it is a structural dependency on entities that have both the means and the motive to exploit it.

Using open-source is a political act

Open-source software is the only technology ecosystem where the power dynamic is reversed: you can verify, modify, and control the tools you rely on.

This is not just about features or cost. It is about whether your digital infrastructure is accountable to you, or to corporations and their political allies.

Open-Source Alternatives That Actually Work

SECTION 4 · ALTERNATIVES

Signal

Communicator

End-to-end encrypted. Open-source protocol. No ads, no data collection, no corporate surveillance. The only trustworthy mass-market messenger.

LibreWolf

Web Browser

Privacy-hardened Firefox fork. Tracking protection enabled by default. No telemetry, no data sharing, no fingerprinting.

K-9 Mail / FairEmail

Mail Client

Open-source mail clients with no data collection. Important note: every email you send through Gmail is read and analysed by Google.

DuckDuckGo

Search & Browser

Does not track searches or build profiles. Not open-source, but significantly less invasive than Google. A practical stepping-stone.

Linux

Operating System

The only mainstream operating system where the source code is fully public and auditable. No hidden telemetry, no built-in corporate surveillance.

There Is Nothing Free in Our World

1. Free services = you are the product

If you receive an OS, app, or service for free, you are paying with your personal data — which is profiled and sold for significant profit. Google, Meta, and TikTok exist because your data is worth more than any subscription fee.

2. ~500 PLN for Windows = paying to be exploited

With Windows, you pay for the privilege of being surveilled. That same money invested in a Linux course gives you full control over your system, a genuinely useful skill, and freedom from corporate dependency.

3. Linux isn't free — it costs time

Linux has a learning curve. The cost is not money but time and effort. The investment is worth it: you gain knowledge, control, and an operating system that works for you — not against you.

SECTION 5

Linux Distributions

Choosing your system wisely

Linux Distributions — A Few of the Many

…and hundreds more. Which one is the best?

Linux Distribution Timeline

SECTION 5 · LINUX

The full family tree of Linux distributions — from 1991 to today — is too large to show on a single slide. It maps over 500 distributions across 30+ years of history.

Open Full Timeline on Wikipedia →

https://en.wikipedia.org/wiki/File:Linux_Distribution_Timeline.svg

```
Debian family  →  Ubuntu → Linux Mint, Pop!_OS, elementary OS, Zorin OS…
Red Hat family →  Fedora → CentOS → Rocky Linux, AlmaLinux…
Arch family    →  Manjaro, EndeavourOS, Garuda Linux…
Gentoo family  →  Chrome OS, Funtoo…
Slackware      →  openSUSE, Salix OS…
Independent    →  Void Linux, NixOS, Alpine Linux…
```

What Is the Difference Between Distributions?

SECTION 5 · LINUX

Release Model

Rolling Release

System is constantly updated — no classic version releases.
Arch, Gentoo, Void Linux

Fixed Release

New versions released periodically — migration required between majors.
Debian, Ubuntu, Fedora

Semi-Rolling

Stable base with faster-updating components.
openSUSE Tumbleweed, Manjaro

Package Manager

pacman — Arch Linux & derivatives

Fast, simple — no reverse dependencies

apt — Debian, Ubuntu & derivatives

Easy to use, large repositories

dnf — Fedora, RHEL, CentOS

Better dependency support than apt, but slower

zypper — openSUSE

Advanced features, system snapshots

portage — Gentoo

Source-based — compile everything from scratch

Which Distro Is the Best?

...

I genuinely don't know — and I genuinely don't care.

But I do know which ones are the worst.

Automated Linux Distributions — The Problem

SECTION 5 · LINUX

If you don't know what's going on under the hood, for sure nothing good is happening. Automatic means potentially dangerous.

Why automation is a problem

Nowadays, everyone wants your data — passwords, money, computing power, or something else. When I configure a system from start to finish myself, I know exactly what is running. With automated distributions, I have to trust that someone else configured it correctly and honestly. I don't have that trust.

Three categories of problematic distributions:

1. User-friendly with too much automation
2. Dark Side — opaque and potentially hostile
3. Lazy distros that hide important details

Category 1: User-Friendly but Over-Automated

SECTION 5 · LINUX

These distros do a lot in the background without giving the user full control:

Ubuntu

Collects anonymous telemetry data by default. Can be disabled, but most users never do — because the opt-out is deliberately buried.

Pop!_OS

Automatic driver and update installation simplifies use but can push unverified packages silently.

Zorin OS

Integrated analytics and automatic downloads of some apps without explicit user action.

EndeavourOS & Manjaro

Automatic mirror and update management could expose users to compromised or outdated mirrors.

Category 2: Dark Side Distributions

Some distributions are heavily automated with unclear or suspicious background processes:

Deepin Linux

A beautiful Chinese distribution suspected of transmitting telemetry data to servers in China. The source code is available but the network behaviour has raised serious red flags.

Kylin OS

A Chinese government-sponsored distribution. Fully automated, but it is not at all clear what processes run in the background or what data is sent where.

Windowsfx

Looks like Windows 11 but runs on Ubuntu. The proprietary modifications are unclear — you gain neither Windows compatibility nor Linux transparency.

Category 3: "Lazy" Distros That Hide Too Much

Generally safe, but hides or abstracts important system information from the user:

Linux Mint

While generally secure, it hides kernel updates behind a separate 'Update Manager' level system that discourages users from installing them — a significant security risk.

elementary OS

Very limited user control over the system and updates. Designed for ease of use, but at the cost of transparency and configurability.

Garuda Linux

Based on Arch but automates so many things that the user may not be aware of significant changes happening to the system.

Distributions You Can Trust

For full control over your system, use a distribution where everything is open and configurable from the start.

Arch Linux

Rolling release. You build it yourself from a minimal base. Nothing runs without your explicit decision.

Gentoo

Compile everything from source. Maximum control, maximum transparency. The basis of our course.

Void Linux

Independent, uses runit init system, musl libc option. Minimal and well-audited.

Debian

Rock-stable. 30+ years of reliability. Conservative — security over cutting-edge.

Slackware

Oldest surviving distro (1993). Almost zero automation. If you can run Slackware, you understand Linux.

What We Will Learn in This Course

SECTION 5 · LINUX

We will learn Arch Linux and Gentoo

Phase 1 — Arch Linux

- Installation from scratch
- The Arch Way: explicit, no magic
- Bootloaders & network management
- Package management with pacman
- Xorg, Wayland & desktop environments

Arch forces you to understand every decision. If you can install Arch, you understand Linux.

Phase 2 — Gentoo

- Compile everything from source
- USE flags & hardware optimisation
- The Linux Kernel — the manual way
- Portage package system
- Performance, security, full control

Gentoo is one of the hardest distros to install. Master it and no other distro will feel difficult.

Why Arch or Gentoo? Top 5 Reasons

SECTION 5 · LINUX

gentoo.org · wiki.gentoo.org

1. Flexibility and Customisation

Precisely tailor the system to your hardware and needs. Full control over every component through the Portage tree and source compilation.

2. Performance and Speed

Compile with your own CPU flags and optimisations. The resulting system is genuinely faster than pre-compiled alternatives for your specific hardware.

3. Security

Designed to be secure by default. You control exactly what is installed and how it is configured. No automatic processes you haven't authorised.

4. Community and Support

Some of the most knowledgeable Linux users in the world. Comprehensive documentation and a community that expects you to understand your own system.

5. Innovative Features

Portage with USE flags, per-package compile options, and the Gentoo Handbook. There is nothing like it in the Linux ecosystem for learning and control.

Thank You

That's everything for the moment.

Please keep an eye on Teams. There are a few more things I wanted to share, but I had to cover a PhD defence at the last minute. I will prepare additional materials on MS Teams or record a video for YouTube. I'm very sorry for the incomplete coverage.