

Digital Autonomy



UNSW, Nov. 11, 2025

Bart Jacobs — Radboud University Nijmegen, NL
bart@cs.ru.nl



Digital Autonomy

Where we are, so far

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions



Overview

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions

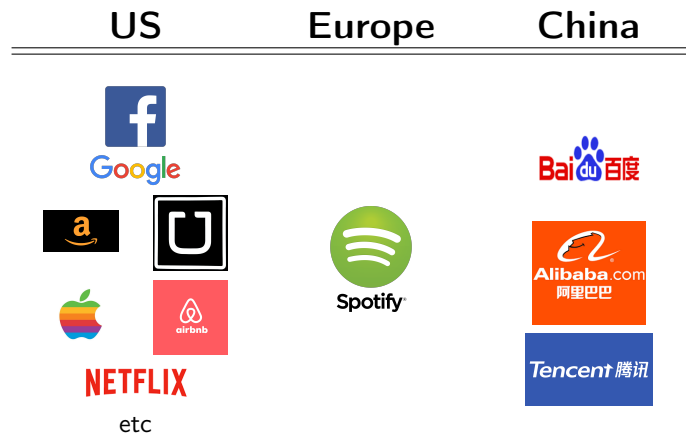


Who is this guy?

- ▶ Professor at Nijmegen (NL), in computer security & privacy
 - studied mathematics & philosophy, ended up in computer science
 - also (formal) appointments in Law & Philosophy
 - member of Royal Academic Society (KNAW) and Stevin-winner
- ▶ Doing a mix of theoretical, practical, societal work
 - in security & privacy a shift towards **usability**
 - with more focus on **sovereignty** and **digital commons**
- ▶ Regular role in media on security/privacy/intelligence issues, and occasionally in parliamentary expert meetings
- ▶ Former member of NL Cyber Security Council (2011 - 2023), and of intelligence evaluation committee (2020)
- ▶ One of the founders of  iHub Nijmegen's interdisciplinary Hub for digitalisation and society, see ihub.ru.nl



Global platforms



EU situation

We run American software on Chinese hardware
(and increasingly, Chinese software too)

Where did we go wrong?



The shared US-CN agenda

- ▶ Both US and CN platforms wish to control digital identities
 - they wish to precisely register who is doing what & when online
 - goal: build up detailed profiles
- ▶ The US platforms have mostly **commercial** motives
 - but they have been used for political manipulation too
- ▶ The CN platforms are instrumental in maintaining **state/CCP control**
 - see e.g. their role in “social credit scores”

These systems work on the basis of a **unique identifier** (number), per individual, that is used everywhere — very unlike attributes (see later)

- ▶ Strong EU sentiment: there are **better ways** to do this, with more respect for human (digital) rights & dignity
- ▶ Decentralised, attribute-based approach combines diversity & easy interoperability: **ideal for EU sovereignty**



EU / NL / Nijmegen / own perspective

- ▶ EU is **regulatory power**, but not a technology power
 - embedding EU values requires stronger digital autonomy
- ▶ **Open source** as a geopolitical instrument, to keep big-tech at bay
 - NL government is focusing stronger on “open, unless”
 - toothless policy, so far, with a few exceptions
- ▶ Serious concerns in various sectors (parliament, banking, academia) about strategic dependence on US cloud
 - calls and cautious initiatives towards local (EU) hosting
- ▶ Nijmegen’s interdisciplinary **iHub** for digitalisation and society
 - with value-driven research agenda and own development/design lab
- ▶ Own team projects with strong “usable security” focus:
 - **Yivi.app**, for attributed-based identity management
 - **PostGuard.eu**, for identity-based encrypted email & file transfer
 - **PubHubs.net**, for a new community network (still early work)



Where we are, so far

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions



Ad 1. Putin's disruption

- ▶ Dutch intelligence chiefs: we're in a **dark grey zone** between war and peace with Russia
- ▶ Putin is actively **disrupting European societies & infrastructure**
 - spoofing GPS, endangering civil aviation
 - large scale cyber attacks, for espionage and sabotage
 - drone incidents, near military and civil airports
 - cutting data/power cables, esp. in Baltic sea
 - physical attack: arson, explosions, murder attempts
 - disinformation, esp. supporting anti-democratic movements
- ▶ An obvious next step if the conflict (with Europe/Ukraine) heats up more is to **cut undersea transatlantic data cables**
 - Russian ships have been monitoring & preparing cable trajectories
 - hard to defend against, high plausible deniability
 - without the cables, hardly anything still works in Europe (what about Australia?)



Main autonomy (disruption) concerns in EU

- (1) **Putin** pulling more sea cables — esp. transatlantic (and Pacific)
 - “smaller” destructions ongoing, esp. in Baltic sea
- (2) **Trump** using IT-dominance for leverage & sanctions (“kill switch”)
 - International Criminal Court (ICC) prosecutor Khan no longer served by Microsoft, after unwelcome Israel investigations
- (3) **Tech-bro's of Trump** dominate our information and decision space
 - with anti-democratic and anti-European agenda
- (4) **European Court of Justice** may (once again) declare EU-US data transfer agreement illegal
 - after succesful “Schrems I” (2015) and “Schrems II” (2020) objections
- (5) **Xi** using rare metals for geopolitical influence
 - also chip-supply (e.g. to car industry) blocked in Nexperia case



Ad 2. Trump's disruption

- ▶ The ICC prosecure cut-off worked as **wake-up call** for many
 - Trump forbids US-companies to provide services to court
 - prosecutor Khan no longer had access to emails, files, etc.
 - decision is **politically motivated** — Israel investigations
 - Microsoft is very unhappy / uncomfortable with the situation
- ▶ ICC decided to **ditch Microsoft** and is switching to open source alternative
 - OpenDesk collaboration platform, via Zendis, hosted in Germany
- ▶ Broader fear of power abuse within current **IT-feudalism**
 - anything that Trump dislikes may be targeted / cut off
 - resulting in growing investments in EU IT-infrastructure
 - **industrial policy** is needed, against abuse of market power / excessive dominance, e.g. via killer acquisitions



Ad 3. Techbro's disruption

- ▶ Big “social” media platforms are instruments for commercial and political manipulation
 - effective targeting and manipulation based on **personal** profiles
 - support for right-wing populists is evident (e.g. Musk and AFD)
- ▶ In this **toxic environment** we still run public **elections** ...
 - platform owners pushing extreme opinions / candidates
 - people are now asking Gen-AI tools for voting advice 😞
 - it is easy to tweak the recommendations
- ▶ Presidential elections Romania (late 2024, early 2025)
 - Out of the blue winner, in first round, campagne via TikTok
 - extreme-right, pro-Russian, critical of EU and NATO
 - Rom. authorities: Russia manipulated the presidential elections
 - Romanian supreme court then excluded this pro-Russian candidate
 - TikTok violating “Digital Services Act” — still under investigation
- ▶ Urgent question: do other countries also have such **emergency breaks**?



Ad 5. Xi's disruption

- ▶ Systematic hacking, largely with economic goals, for own benefit
- ▶ Concerns about back-doors and kill switches in advanced products (GSM, cars, batteries, solar panels)
 - also about data collection for manipulation — esp. via TikTok
- ▶ Increasing strategic use of its production & resource dominance
 - CN's economic power is used for geopolitical goals
 - not discussed further here



Ad 4. CJEU's disruption / protection

- ▶ Europe's data-protection laws (“General Data Protection Regulation”, GDPR) in principle **forbids** processing of personal data of European citizens **outside EU**
- ▶ Special arrangements can be needed, guaranteeing a similar level of protection, such as **EU-US-privacy shield**
- ▶ Still, US intelligence agencies have access to the data
 - privacy activist Max Schrems has successfully contested these arrangements in EU-courts: inadequate protection for EU citizens from government surveillance
- ▶ Latest fix under Biden is “Data Protection Court of Review”
 - Trump is undermining it, strengthening contestants in EU courts
 - US cloud may be declared **illegal** by European judges
 - (first attempt by French MP Latombe failed recently)



Painful question

How did we let such controversial actors take total control over our information and decision space — making it such a hostile environment, so at odds with basic European values (like privacy and dignity)?

- ▶ Naivety, laziness, convenience, indolence, stupidity
- ▶ Maybe more important: *how do we get out of there?*
- ▶ I offer no solutions, at most some, **separate directions**:
 - (1) invest in own decent alternatives — and use them too
 - (2) **regulate** even more strictly, and even **forbid** certain “social” media
 - (3) hardening of our ICT-infrastructure
 - (4) stop being naive, for a resilient democracy
 - (5) ...

I will expand on “alternatives” and “hardening”, in relation to my own work



Where we are, so far

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions

General remarks about Yivi.app

- ▶ Started around 2010, as academic research project, called “IRMA”
 - crypto-basis: zero-knowledge proofs, from Idemix (IBM, Zürich)
 - also for identifying attributes, like full name, email, mobile nr.
 - with smart card (first) and phone app (later) prototypes
 - new concept: **proportional authentication** — with data minimalisation
- ▶ In 2015 Yivi moved out of academia, to non-profit spin-off
 - called [privacybydesign.foundation](#)
 - roll-out 2019-24 with SIDN, non-profit domain registrar in NL
 - 2024-now, with commercial NL company **Caesar Group**
 - some academic Yivi research remains at university, e.g. on voting
- ▶ Hugely influential, e.g. copied by EU in their **wallet-ID** plans
 - working app has been **eye-opener** for policy makers & others
 - **Message**: things can be done differently, there is a (political) choice, esp. relevant now for **EU digital autonomy**.



Current cooperation with company Caesar

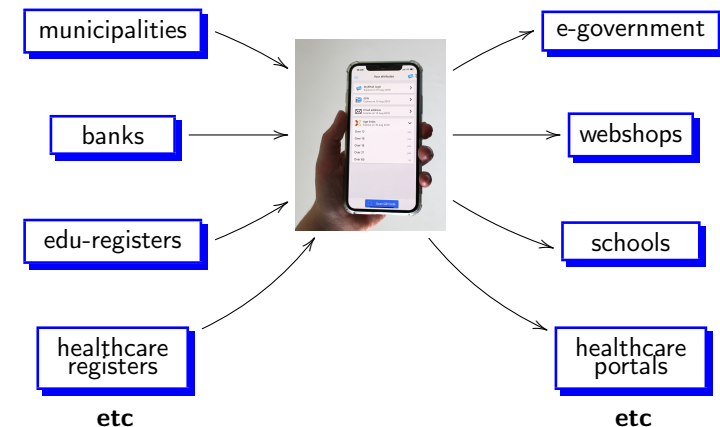
- ▶ The privacy by design **foundation** holds Yivi brand rights
 - and also web addresses like yivi.app and yivi.nl
 - the foundation is non-profit and does *not* have own employees
- ▶ Caesar is family-owned, Dutch IT-**company**, with ±150 employees
- ▶ The foundation and Caesar have signed a **contract**, saying in essence:
 - Caesar gets exclusive rights to (commercially) exploit Yivi brand
 - they run the infrastructure (backend servers, app) with EU hosting
 - they keep Yivi open source, privacy-friendly & secure, free for end-users
 - strategic decisions are taken jointly.
- ▶ The aim is to combine **public values** with **corporate efficiency**
 - this works really well, so far, but not yet a commercial success



The Yivi app as everyone's personal hub

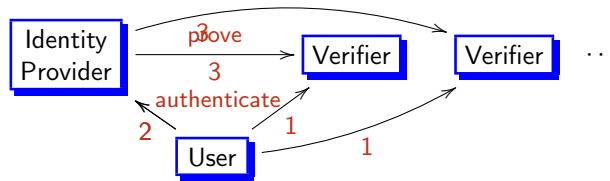
attribute sources

attribute receivers

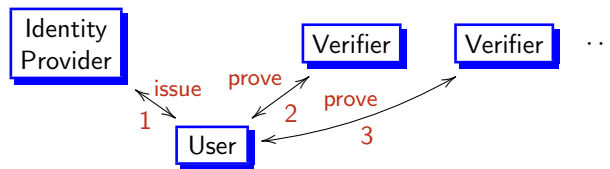


Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook)



Decentralised: everything goes via the User (think Yivi)



Note: Data flows determine power relations in modern societies!



Yivi applications, so far

- ▶ General remark: up-take is slow — for all identity wallets
 - commercial parties fear losing customers — because of friction
 - applications mostly via obligations or added functionality
- ▶ Actual Yivi applications e.g. in local government, health, insurance
 - estimated number of users $\geq 100K$
- ▶ Potential new big international area: privacy-friendly, open source age verification for “social” media and XXX sites
 - much political pressure, but also resistance among population
 - data minimisation via attributes may be way out
 - reveal only “over 16” or “over 18” attributes
- ▶ Australia plays leading role in age verification
 - but disappointingly, has left verification technology up to Big-Tech
- ▶ Yivi now supports attribute-loading via passports: **do try it yourself!**
 - Yivi globally offers privacy-friendly open source age verification!
 - pass it on!



Yivi as enabler: PostGuard, part I

- ▶ Digital identity is often the starting point of security solutions
 - that’s why digital identity is of such geopolitical relevance
 - it is part of “hardening our infrastructure”
- ▶ Cool technology: identity-based encryption and signing
 - developed by Shamir, Boneh, Franklin
 - public key is derived from individual identity
 - private key comes from key-generator server (“KGS”), after identity check
 - greatly simplifies key management
 - it is also more understandable, with better mental model
- ▶ Implementation via Yivi — described for encryption first
 - sender of file chooses attributes of receiver: email, mobile, name, ...
 - public key for encryption is derived locally, from these attributes
 - receiver proves identity to KGS, then gets decryption key
 - signing can be done dually — and can be combined with encryption



Yivi as enabler: PostGuard, part II

- ▶ PostGuard exists as academic prototype, see postguard.eu
 - It is now being professionalised to a security product
- ▶ Usability receives explicit attention
 - encryption is a difficult concept for many people
 - not easy to explain, certainly not its key management
- ▶ PostGuard guarantee: only the intended recipient can see the message.
 - this is what people wish to be certain about
- ▶ Alternatives for WeTransfer and DropBox (from US) badly needed
 - they offer little security, have access to the data themselves
 - plans to use data for AI-training withdrawn for now under pressure



Digital identity as further enabler: authenticity

- ▶ Our information space is flooded with mis/dis-information, increasingly AI-generated
- ▶ Deliberate strategy: *flooding the zone with bullshit* (Steve Bannon)
 - the aim is **reality fatigue** among the population
 - so that people give up trying to find out what is true or not
 - actively undermining informed democratic debates
- ▶ Own proposal: focus on **authenticity** of information
 - i.e. certainty about source and integrity
 - this is not the same as truth
 - great mechanism: **digital signature**
 - this can strengthen institutions online
 - but it may also be essential for AI, via authentic training data
 - see article [The Authenticity Crisis](#) (Comp. Law Security Rev, 2024)
- ▶ Identity wallets (like Yivi) can be enabler for flexible **role-based signing**



Where we are, so far

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions



Disruption through “social” media

- ▶ Current “social” networks have devastating societal effects
 - fake news, extremism, polarisation, all via engagement optimisation
- ▶ Attention economy leads to **radicalisation** and **polarisation**
 - Jaron Lanier: X/Twitter is an “asshole amplification network”
- ▶ Toxic environment for (well-meaning) public office holders, politicians, experts, esp. for women and minorities
 - undermining content-driven democratic debate
- ▶ Based on extreme interpretation of freedom of speech
 - not on human **dignity** and quality of debate
- ▶ In everybody’s pocket, basis for “news” and personal judgements



Own “hardening” work on PubHubs

- ▶ New community platform [PubHubs.net](#) based on public values
 - aim is combination of **privacy** and **accountability**
 - via flexible digital identities (with own eID wallet Yivi)
 - including digital signatures
 - for respectful, decent contact with (and in) rank and file of organisations
 - at this stage running pilots, broader launch later this year
- ▶ Such independent, locally-hosted platforms are important for:
 - digital sovereignty, continuity of business
 - whole-of-society approaches in crisis situations
- ▶ Also relevant for discussions about **minors** and “social” media
 - when there are decent alternatives, restricting access to dubious platforms is less dramatic

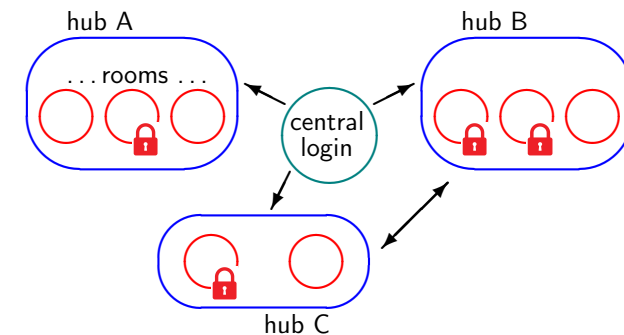


PubHubs and digital identity

- ▶ Digital identity is a crucial part of PubHubs
 - for central login, and also for “secure” rooms in hubs
 - e.g. for disclosing your postal code for neighbourhood room
- ▶ Identity is an instrument for **moderation**, and accountability
 - e.g. a misbehaving user may need to disclose their real name
 - ultimately it is used for exclusion — requiring persistency
 - users may be banned from rooms / hubs / PubHubs
- ▶ Therefore, standard social logins do not work for PubHubs
 - also, Matrix logins do not give access
 - nor Fediverse / ActivityPub

See *PubHubs Identity Management* publication: doi.org/10.1093/logcom/exad062

PubHubs high-level picture



- ▶ Once logged in (centrally), users can freely move between hubs
- ▶ Users automatically get different pseudonyms in different rooms
- ▶ Access restrictions may apply to rooms within hubs
- ▶ This infrastructure is up-and-running — but only for Europe so far



Where we are, so far

Introduction

Autonomy disruptions

Yivi identity wallet

Social media for the public good

Conclusions

Concluding remarks

- ▶ Re-election of Trump has made existing IT-feudalism **really visible and problematic**
- ▶ IT-sector dominated by super-powerful private parties
 - no level playing field, no functioning market — see killer acquisitions — highly problematic political agenda
 - Europe has to start playing on a different chess-board
 - with **open source** as counter strategy, avoiding lock-ins
 - Australia could be a natural partner in this
- ▶ European IT-reorientation also offers **opportunities**
 - rebuild IT based on public / European values
 - academics have role to play — e.g. with prototypes
- ▶ Own work esp. in **digital identity** — with applications
 - Broader message: there are alternative approaches, there is a choice!



Thanks for your attention. Questions/remarks?

