# Platform Sovereignty and Digital Identity

Alex Applebee & L. N. Combe

2026

# Platform Sovereignty and the Privatisation of Human Identity

## A Unified Thesis on Corporate Identity Monopolies, Surveillance Capitalism, and the Case for Sovereign Infrastructure

**Authors:** Alex Applebee and L. N. Combe

**OMXUS Research Series – Papers 22 & 23 (Unified)**

---

## Author's Note

This document exists because of Goal 8: *Internet costs nothing. You ARE the infrastructure.*

The argument you are about to read is not abstract. It has a working implementation.

The OMXUS identity system derives your cryptographic identity entirely client-side – from your name, your date of birth, and secret words you choose. The seed phrase never leaves your browser. No server ever sees it. The same inputs produce the same identity on any device, in any country, forever. No account creation. No email verification. No company in the middle.

The network layer beneath it – BLE mesh, WiFi direct, LoRa – means your device is a node. You do not connect to the internet. You are the internet. When you walk into a room, the network gets stronger. When you leave, the network walks with you. No ISP bill. No fibre to the premises. No Telstra. No Comcast. No permission.

These are not proposals. They are running code. The identity derivation is 47KB of JavaScript. The mesh protocol is a BLE advertisement. The emergency response system is a $29 ring.

We wrote this thesis because the academic literature documents the disease but prescribes nothing. Zuboff named surveillance capitalism. Couldry named data colonialism. Halpern named the smartness mandate. None of them built the exit. This paper names the disease and opens the door.

If you are reading this and you work at Google, Apple, Meta, GitHub, or Microsoft: the system you maintain is not a service. It is a cage with a colourful logo. The people inside it did not choose to be there. They clicked a button twenty years ago and you kept building walls around them. This paper is the blueprint for the door.

If you are reading this and you are Bill from Geelong, or someone like him: your identity does not belong to a company in California. It belongs to you and the people who can see your face. Four people in a room. That is all it takes.

– A.A. & L.N.C.

---


## Abstract

Five corporations – Google, Apple, Meta, GitHub, and Microsoft – function as de facto identity authorities for the majority of the world's digital population. Their combined annual revenue exceeds $1.037 trillion, funded primarily by monetising identity data that users provided without meaningful consent. This thesis synthesises the academic frameworks of surveillance capitalism (Zuboff, 2019), data colonialism (Couldry & Mejias, 2018), the smartness mandate (Halpern & Mitchell, 2022), and planetary surveillance (Pasquinelli, 2023) to demonstrate that corporate identity monopoly is not an accident of market dynamics but a structural feature of platform economics. We document the mechanism of identity privatisation through the "convenience trap" – a twenty-year sequence of individually rational decisions that produced collective captivity. We present empirical evidence of de-platforming as identity death through four documented cases: a father criminalised for medical photos of his child, a 25-year Apple customer locked out over a compromised gift card, blanket restriction of developers by nationality, and mass deletion of inactive accounts. We examine the self-sovereign identity (SSI) movement and explain why its technical solutions have failed to achieve adoption. We propose and describe a working alternative: mutual physical attestation combined with client-side cryptographic identity derivation and peer-to-peer mesh networking – infrastructure that requires no corporation, no server, and no permission. The system described is not theoretical. It is deployed.



**Keywords:** digital identity, platform dependency, identity sovereignty, corporate gatekeeping, de-platforming, authentication monopoly, surveillance capitalism, data colonialism, smartness mandate, self-sovereign identity, decentralised identifiers, mesh networking, VexID, physical attestation


---

## Table of Contents


1. Foreword: Goal 8 and the Shape of the Exit
2. Chapter 1: Introduction – The Thought Experiment
3. Chapter 2: The Five Gates
4. Chapter 3: How Identity Got Privatised
5. Chapter 4: The Cost of Corporate Identity
6. Chapter 5: Literature Review – Surveillance Capitalism and the Identity Bargain
7. Chapter 6: Data Colonialism and the Smartness Mandate
8. Chapter 7: De-Platforming, Digital Death, and the Academic Blind Spot
9. Chapter 8: Self-Sovereign Identity – Why the Technical Solution Failed
10. Chapter 9: The Alternative – Physical Attestation and Sovereign Infrastructure
11. Chapter 10: VexID – Implementation Architecture
12. Chapter 11: Mesh Networking – You Are the Infrastructure
13. Chapter 12: The Permission We Gave

14. Chapter 13: Who Owns You? – The Kitchen-Table Version
15. Chapter 14: Bill
16. References
17. Appendix A: Key Statistics
18. Appendix B: Cross-References to OMXUS Research Series
19. Appendix C: Image Inventory

---

## Foreword: Goal 8 and the Shape of the Exit

> *"Internet costs nothing. You ARE the infrastructure. Mesh networking. No ISP required. BLE, WiFi, LoRa – your device is a node."* – OMXUS Goal 8

The fourteen goals that drive the OMXUS project were not designed by committee. They come from grief, injustice, and lived experience of system failure. Each one traces to a system that broke a real person. They are prevention requirements.

Goal 8 says the internet should cost nothing. Not subsidised. Not discounted. Nothing. Because the infrastructure already exists in your pocket. Every phone manufactured in the last decade contains Bluetooth Low Energy, WiFi, and a processor capable of cryptographic operations. These devices can communicate directly with each other – peer to peer, no tower, no cable, no ISP, no monthly bill. They do not because the companies that sell connectivity have no incentive to enable free connectivity. And the companies that sell identity have no incentive to enable free identity.

This thesis addresses both. The identity monopoly documented in these pages cannot be broken by building a better login page. It can only be broken by removing the need for a login page entirely. Client-side identity derivation – where your cryptographic keypair is generated from inputs you memorise, never transmitted, never stored on a server – eliminates the identity layer that five companies sit on top of. Mesh networking – where your device routes packets for your neighbours and their devices route packets for you – eliminates the infrastructure layer that ISPs sit on top of.

Together, they answer Goal 8. The internet costs nothing because you are the internet. Your identity costs nothing because your identity is you.

The academic literature we review in this thesis documents the problem with precision and prescribes nothing. This thesis documents the problem and opens the door.

---

## Chapter 1: Introduction – The Thought Experiment

Try a thought experiment. Imagine your Google account disappeared tomorrow. Not deactivated – gone.

Your email is gone. Every account that uses "Sign in with Google" is locked. Your photos – every photo you've taken on an Android phone for the last decade – are gone. Your calendar, your contacts, your documents. Your YouTube history, which at this point knows you better than your therapist. Your Google Authenticator tokens, which means every other account protected by 2FA is now inaccessible. If you have an Android phone, it is now a brick.

You didn't die. But digitally, you ceased to exist.

One company. One decision. One button.

Now consider: Google doesn't even need to press the button. You will never do anything to risk them pressing it. That's the power. Not the action – the threat. You self-censor, self-moderate, self-comply, because the alternative is digital death. And you agreed to this. Paragraph 47 of a terms of service document that no human has ever read in full.

This thesis examines how five corporations assumed control of human identity, what that control costs, and why the alternative – mutual physical attestation between humans, backed by client-side cryptography and peer-to-peer networking – requires no corporation at all.

---

## Chapter 2: The Five Gates

### 2.1 Google: The Default Identity

Google accounts: 1.8 billion+ (Statista, 2024). Android market share: 71.8% globally (StatCounter, 2024). Gmail market share: 29.7% of all email clients (Litmus, 2024).

Google is not an email provider. Google is an identity provider that happens to offer email. "Sign in with Google" is the most widely used authentication method on the internet. When a startup builds a login page, the first button is Google. Not because Google is best – because Google is default.

What Google controls:

- **Email** – and therefore password resets for every other service
- **Authentication** – Google Authenticator, Google Sign-In, Google OAuth
- **Storage** – Google Drive, Google Photos (over 4 trillion photos stored)
- **Communication** – Gmail, Google Meet, Google Chat
- **Navigation** – Google Maps (where you go, when, how often)
- **Knowledge** – Google Search (what you ask, what you want to know)
- **Device activation** – Android phones require a Google account to function
- **App distribution** – Google Play Store controls what software 71.8% of phones can run

Banning a Google account is not a terms of service enforcement action. It is an identity execution.

### 2.2 Apple: The Walled Garden as Identity

Active Apple devices: 2.2 billion (Apple, 2023). iCloud users: 850 million+.

Apple's identity control is architectural. Your iPhone is not your phone – it is Apple's phone that you are permitted to use under licence. Apple can:

- **Disable your device** remotely (kill switch since iOS 7)
- **Remove apps** from your phone retroactively (done with Fortnite, 2020)
- **Block sideloading** – you cannot install software Apple hasn't approved (until DMA enforcement, EU only)
- **Control payments** – Apple Pay, in-app purchases, subscriptions all route through Apple
- **Lock your data** – iCloud encryption keys are held by Apple, not you (except Advanced Data Protection, opt-in, 2022)

Apple's App Store Review Guidelines are 30 pages of rules about what software is permitted to exist. Not what software is legal – what software Apple approves of. In 2024, Apple rejected or removed

apps for: competing with Apple services, displaying content Apple deemed objectionable, using payment systems that bypass Apple's 30% commission, and offering functionality Apple planned to build itself.

Apple is not a phone company. Apple is a permission company.

### 2.3 Meta: The Social Graph as Identity

Monthly active users across Meta platforms: 3.74 billion (Meta, 2024). That is 46% of all humans alive.

Meta doesn't control your identity in the Google/Apple sense. Meta controls something more fundamental: your relationships. Your social graph – who you know, how you know them, how often you interact, what you say to each other – exists on Meta's servers. Not yours.

When Meta disables an account:

- Your Messenger history with every person you've communicated with: gone
- Your Facebook groups (many of which are the only community infrastructure for isolated people): gone
- Your Instagram presence (for many small businesses, their only storefront): gone
- Your WhatsApp (2 billion users, default communication in much of the developing world): gone

In 2021, Facebook went down for 6 hours. In countries where WhatsApp is the default communication infrastructure – India, Brazil, much of Africa – the outage disrupted government services, healthcare coordination, and emergency communication (BBC, 2021). Six hours. One company's server outage caused a communications blackout across the developing world.

Meta is not a social network. Meta is a communications monopoly that captured the social graph of half the planet.

### 2.4 GitHub: The Code Gate

GitHub users: 100 million+ (GitHub, 2023). Repositories: 330 million+.

GitHub's identity monopoly is narrower but more consequential per capita. GitHub controls:

- **Professional identity** for software developers – your GitHub profile is your resume
- **Code hosting** – the majority of open-source software is hosted on GitHub
- **Collaboration infrastructure** – Issues, Pull Requests, Actions (CI/CD)
- **Dependency distribution** – npm (JavaScript), NuGet (.NET), Packages (multiple languages)
- **Copilot** – AI code generation trained on repositories hosted on GitHub

In 2019, GitHub restricted accounts from Iran, Syria, Crimea, Cuba, and North Korea due to US trade sanctions (GitHub, 2019). Developers in those countries lost access to their own code. Not because they violated any terms of service. Because of where they were born.

GitHub is owned by Microsoft (acquired 2018, $7.5 billion). The company that controls the operating system of 72% of desktop computers also controls the platform where most software is built.

### 2.5 Microsoft: The Enterprise Identity

Microsoft 365 users: 1.2 billion+ (Microsoft, 2024). Azure Active Directory (Entra ID) authentications: 1.2 billion per day.

Microsoft's identity control operates primarily through enterprise:

- **Azure Active Directory** (now Entra ID) is the identity provider for most corporate environments
- **Microsoft 365** controls email, documents, communication, and calendars for most businesses
- **Windows** – 72% desktop market share – increasingly requires a Microsoft account
- **LinkedIn** – professional identity and job seeking for 1 billion users
- **GitHub** – see above

Microsoft is the company most people don't think of as an identity company. That's what makes it the most powerful one. Your employer uses Microsoft. Your employer's IT department controls your Microsoft account. Your Microsoft account controls your access to your job. Your job controls your income. Your income controls your housing, food, and healthcare.

The chain is: Microsoft -> IT admin -> your employment -> your survival.

### 2.6 The Unelected Government

These five companies collectively control:

| Function | Government Equivalent | Corporate Controller |
|---|---|---|
| Identity documents | Passport office | Google, Apple |
| Communications infrastructure | Postal service, telecom | Meta, Google, Microsoft |
| Currency/payments | Central bank, treasury | Apple Pay, Google Pay |
| Software distribution | – | Apple App Store, Google Play |
| Professional credentials | Licensing boards | LinkedIn, GitHub |
| Public square | Town hall | Meta, Twitter/X |
| Surveillance | Intelligence agencies | All of them |

No election. No constitution. No bill of rights. No appeals court (Meta's "Oversight Board" is an advisory body with no binding authority). No democratic mandate of any kind.

The US government needs a warrant to read your email. Google reads every email to serve you ads. You agreed to it in the terms of service you never read.

---

## Chapter 3: How Identity Got Privatised

### 3.1 The Convenience Trap

Nick Couldry and Ulises Mejias describe what is happening here as "data colonialism" – a process that transforms "lived experience into abstract, commodifiable data points" (Couldry & Mejias,

2018). The parallel to historical colonialism is structural: where empires used military force to extract land and labour, platforms use convenience to extract behavioural data. The "civilizing mission" is now "becoming smart" (Halpern & Mitchell, 2022). The consent mechanism is no longer the gun – it's the login page.

Nobody handed Google their identity on purpose. It happened through convenience.

- **2004:** Gmail launches. Free email with 1GB storage (Hotmail offered 2MB). You sign up.
- **2007:** iPhone launches. You create an Apple ID to download apps.
- **2008:** Facebook opens to everyone. You sign up to see college photos.
- **2008:** GitHub launches. You host your first project.
- **2011:** "Sign in with Google/Facebook" appears. You click it because it's easier than creating another password.
- **2015:** Two-factor authentication. You add your phone number to Google. Now Google has your phone number, your email, your identity, and your authentication.
- **2020:** Pandemic. Everything moves online. Your Google/Apple/Microsoft account becomes the only way to work, learn, and communicate.
- **2024:** Your entire digital existence – 20 years of photos, emails, documents, relationships, professional history – lives on servers you don't control, under terms you didn't read, governed by companies you didn't choose.

Each step was individually rational. The aggregate is captivity.

### 3.2 The Authentication Monopoly

"Sign in with Google" is not a feature. It is an identity monopoly masquerading as convenience.

When a website offers "Sign in with Google," it is outsourcing its identity verification to Google. The user never creates an account with the website – they authenticate through Google. This means:

- Google knows every service you use
- Google controls your access to every service
- If Google disables your account, every "Sign in with Google" service is inaccessible
- The service has no independent relationship with you – only with Google's representation of you

OAuth was designed as a delegation protocol: "let this app access my Google data." It became an identity protocol: "Google says I'm real, so I'm real." The distinction matters. In the delegation model, you have an identity and Google helps you share it. In the identity model, Google *is* your identity.

### 3.3 The Protocol Capture

The technical history illuminates the political economy. OAuth 2.0 (RFC 6749, 2012) was designed as an authorisation framework – a way for a user to grant limited access to their resources on one service to another service. It was explicitly not an authentication protocol. OpenID Connect (2014) layered authentication on top of OAuth 2.0, creating the "Sign in with…" pattern. The distinction between authorisation ("let this app see my photos") and authentication ("this person is who they claim to be") was collapsed.

This collapse was not accidental. It was profitable. When authentication flows through Google, Google becomes the chokepoint for identity. Every service that implements "Sign in with Google" adds another bar to the cage. Every user who clicks the button adds another data point to the behavioural surplus that funds $307 billion in annual advertising revenue.

The open-source community built the protocols. The corporations captured them. OAuth was a key. Google turned it into a lock.

---

## Chapter 4: The Cost of Corporate Identity

### 4.1 De-Platforming as Digital Death

When a platform bans a user, the consequences extend far beyond that platform:

- **Google ban** -> loss of email, 2FA, cloud storage, device functionality, all "Sign in with Google" accounts
- **Apple ban** -> device potentially disabled, all purchases (apps, music, books) revoked, iCloud data inaccessible
- **Meta ban** -> loss of social connections, communication history, community membership, small business storefront
- **GitHub ban** -> loss of professional portfolio, code history, open-source contributions, CI/CD pipelines
- **Microsoft ban** -> loss of corporate email, documents, job access, LinkedIn profile

There is no due process. There is no appeal with guaranteed timeline. There is no public defender. There is no presumption of innocence. There is a terms of service agreement and a button.

These are not hypothetical scenarios. They are documented.

**Mark, San Francisco, 2021.** During the pandemic, Mark's toddler developed a groin infection. His nurse asked him to photograph it for a telehealth consultation – standard practice when doctors weren't seeing patients in person. He took the photos on his Android phone. Google's automated CSAM detection flagged the images and locked his account. Two days later, Mark lost his email, his photos, his cloud storage, his authentication. Google also reported him to the San Francisco Police Department, who opened an investigation and served search warrants on Google and his ISP. The police investigated and cleared him – this was a father following a nurse's medical instructions. Google refused to reinstate his account. Mark appealed twice. Google's response: the images constituted "harmful content" and a "severe violation of Google's policies" (Fung, 2022; 9to5Google, 2022). A father photographed his sick child because a nurse told him to. The police cleared him. Google didn't care. His digital life – years of email, photos, documents, authentication – remained gone.

**Dr. Paris Buttfield-Addison, 2025.** A software developer and author who had held an Apple ID for 25 years. He purchased an Apple Gift Card from a major retailer. The code was compromised – not by him, by whoever handled the card before he bought it. The retailer reissued a replacement code, which he redeemed. Apple locked his entire account. His Macs, iPhone, iPad, and Apple Watch stopped functioning properly – they couldn't sync, update, or activate. Terabytes of family photos became inaccessible. His message history, his work documents, his app purchases spanning two decades – gone. Apple Support told him nothing could be done and refused to explain why the account was locked. They suggested he "create a new account and start fresh," abandoning

thousands of dollars in purchases and 25 years of data. The account was only restored after the story went viral and reached Apple Executive Relations (Buttfield-Addison, 2025; AppleInsider, 2025). Without media attention, a 25-year customer would have lost everything because a retailer sold him a compromised gift card.

**Iranian, Syrian, and Crimean developers, 2019.** In July 2019, GitHub restricted private repositories and paid accounts for developers in Iran, Syria, Crimea, Cuba, and North Korea. No prior notice. Developers discovered their accounts were blocked with no option to download their own code. An Iranian developer's Medium post describing the lockout went viral. GitHub CEO Nat Friedman acknowledged the pain: "It is painful for me to hear how trade restrictions have hurt people" (TechCrunch, 2019). GitHub later worked with the US Treasury to restore some access to Iranian developers, but the precedent stands: your professional history, your code, your portfolio exist at the pleasure of a company in San Francisco, and that company answers to a government you don't vote for.

**Google inactive account purge, 2023.** On December 1, 2023, Google began deleting accounts that had been inactive for two years. All content – Gmail, Drive, Photos, everything – permanently erased (NPR, 2023). Google's security rationale was reasonable: inactive accounts are more vulnerable to compromise. But "inactive" does not mean "unwanted." It means the person stopped logging in. Maybe they switched to a different phone. Maybe they got sick. Maybe they died and their family hadn't thought to log in. The photos, the emails, the documents – gone. Not because anyone did anything wrong. Because nobody logged in for 24 months.

Each of these cases follows the same pattern. An ordinary person – not a political figure, not a public threat, not a criminal – loses their digital identity through a process they cannot see, cannot challenge, and cannot reverse. The system that decides whether they exist has no judge, no jury, and no obligation to explain itself.

### 4.2 The Data Asymmetry

Google knows:

- Every search you've made (knowledge, desires, fears)
- Every email you've sent and received (relationships, commitments, secrets)
- Every place you've been (Google Maps, location history)
- Every purchase you've made (Gmail receipt scanning)
- Every app you've used (Android, Play Store)
- Your face (Google Photos facial recognition)
- Your voice (Google Assistant recordings)
- Your fingerprint (Android biometrics)
- Every website you've visited (Chrome, the world's most popular browser)

You know about Google:

- It has a colorful logo.

This is not a symmetric relationship. This is not a transaction. This is surveillance exchanged for convenience, and the price was set by the company providing the convenience.

### 4.3 What It Costs in Money

Google revenue 2023: $307 billion. Primarily from advertising – selling predictions about your behaviour to companies that want to modify your behaviour (Zuboff, 2019). Matteo Pasquinelli describes this as a "planetary business of surveillance and forecasting" (Pasquinelli, 2023, p. 12) – the extraction of behavioural patterns at civilisational scale, repackaged as a free service.

Apple revenue 2023: $383 billion. Including 30% commission on all App Store transactions – a tax on software that no government voted for.

Meta revenue 2023: $135 billion. Almost entirely advertising – the social graph of 3.7 billion humans, monetised.

Microsoft revenue 2023: $212 billion. Enterprise software and cloud – your employer pays Microsoft for the right to control your work identity.

Combined: **$1.037 trillion per year.** Funded by monetising identity data that users provided for free.

### 4.4 The Attention Economy Connection

The identity monopoly does not operate in isolation. It intersects with and reinforces the attention economy documented in the OMXUS screens and attention economy research. The same companies that control identity also control attention: Google owns YouTube (2.7 billion monthly users), Meta owns Instagram and Facebook (3.74 billion combined), Apple controls the App Store through which attention-harvesting applications are distributed. Identity lock-in ensures that even when users recognise the harm of attention extraction, they cannot leave. Your photos are on Google. Your friends are on Meta. Your apps are on Apple. The cost of reclaiming your attention is the loss of your identity. This is not a coincidence. It is architecture.

---

## Chapter 5: Literature Review – Surveillance Capitalism and the Identity Bargain

### 5.1 Zuboff and the Extraction Logic

Shoshana Zuboff's *The Age of Surveillance Capitalism* (2019) established the foundational framework for understanding how technology companies monetise human behaviour. Zuboff argues that Google pioneered a new economic logic: extracting "behavioural surplus" from user activity to generate predictions about future behaviour, then selling those predictions to advertisers. The key insight is that this extraction requires identity – without knowing who you are, prediction markets collapse. Users provide their identity for free, and the company sells predictions derived from it for $307 billion per year. Zuboff coined the term "surveillance capitalism" but her analysis focuses on the advertising model. What she does not fully examine is the identity lock-in that makes the advertising model possible. "Sign in with Google" is not just a convenience feature – it is the mechanism by which Google ensures you cannot leave. Every service authenticated through Google becomes another bar in the cage.

Zuboff's framework is necessary but insufficient. She documents what the machine does. She does not document what happens when you try to unplug from it. The de-platforming cases in Chapter 4 fill that gap.

### 5.2 The Behavioural Surplus Pipeline

Zuboff identifies a pipeline: raw behavioural data -> behavioural surplus (data beyond what is needed for service improvement) -> prediction products -> behavioural futures markets. Identity is the key that makes this pipeline function. Without persistent identity, behavioural data is noise. With persistent identity, it is a product worth $307 billion annually.

The pipeline has a corollary that Zuboff notes but does not fully develop: the platform must ensure that identity remains persistent. If users could easily create, discard, and recreate identities, the behavioural surplus would fragment. "Sign in with Google" solves this problem for Google. It creates identity persistence across the entire web, not just within Google's own services. Every website that implements Google OAuth contributes behavioural data back to Google's prediction engine, whether the website operator intends this or not.

---

## Chapter 6: Data Colonialism and the Smartness Mandate

### 6.1 Couldry, Mejias, and the Colonial Structure

Nick Couldry and Ulises Mejias (2018) extend the analysis by framing platform identity extraction as colonialism. Their argument is structural: just as historical colonial powers extracted raw materials from colonised populations, digital platforms extract behavioural data from users. The "consent" mechanism – a terms of service agreement nobody reads – parallels the treaties colonial powers used to legitimate extraction. The authors describe how "lived experience" is transformed into "abstract, commodifiable data points" (p. 338). Applied to identity: your name, your face, your location, your relationships, your habits are all raw materials extracted without meaningful consent and refined into products sold to third parties. The colonial parallel is not metaphor. It is structure. The login page is the port of entry.

### 6.2 Halpern, Mitchell, and the Mandate

Orit Halpern and Robert Mitchell's *The Smartness Mandate* (2022) identifies a broader ideological frame: the assumption that computational optimisation of human life is both inevitable and desirable. "Becoming smart" – smart cities, smart homes, smart devices – requires handing behavioural data to platforms that promise to make your life more efficient. The mandate is not optional. Try buying a phone without creating a Google or Apple account. Try applying for a job without LinkedIn. Try communicating in Brazil without WhatsApp. The authors argue that "smartness" functions as a civilising mission – the contemporary equivalent of colonial narratives about bringing progress to backward populations. The identity trade-off is presented as obvious: of course you would give Google your data in exchange for a better search engine. Of course you would let Apple control your phone in exchange for a smoother experience. The alternative – managing your own identity – is framed as primitive.

This framing is the cage's paint job. The bars are structural. The paint makes them look like a feature.

### 6.3 Pasquinelli and Planetary Surveillance

Matteo Pasquinelli's *The Eye of the Master* (2023) provides the political economy. He describes the platform model as a "planetary business of surveillance and forecasting" (p. 12) – not a set of

individual companies but a global system of behavioural extraction operating at civilisational scale. Pasquinelli traces this back to the division of labour: automation does not eliminate work but makes work invisible while making surveillance visible. Applied to identity: your Google account is a labour-extraction device. You perform the labour of self-identification, data generation, and behavioural consistency. Google extracts the value. The fact that you don't get paid for this labour – that you pay for it with your identity – is the innovation.

### 6.4 Synthesis: The Identity Tax

Taken together, these four frameworks – Zuboff's behavioural surplus, Couldry and Mejias' data colonialism, Halpern and Mitchell's smartness mandate, and Pasquinelli's planetary surveillance – describe a single phenomenon from four angles. The phenomenon is this: five companies have imposed an identity tax on the digital population of Earth. The tax is not monetary. It is existential. You pay with your data, your autonomy, your attention, and your right to exist without permission. The combined revenue from this tax is $1.037 trillion per year. No government levied it. No electorate approved it. No court reviewed it. It was imposed through login pages and accepted through convenience.

---

## Chapter 7: De-Platforming, Digital Death, and the Academic Blind Spot

### 7.1 The Literature's Focus

The academic literature on de-platforming focuses primarily on public figures and political speech (Rogers, 2020; Jhaver et al., 2021). Jhaver and colleagues examined the effectiveness of de-platforming as a moderation strategy on Twitter, measuring changes in toxicity after high-profile account suspensions. Rogers tracked the migration of de-platformed extremists to Telegram and alternative social media. These studies are valuable but narrow: they examine de-platforming as a speech act, not as an identity act.

What remains underexamined is the identity death that accompanies de-platforming for ordinary users. A banned Google account does not merely silence someone's political speech. It destroys their email, their authentication, their photos, their calendar, and potentially their phone. Tarleton Gillespie's *Custodians of the Internet* (2018) documents how platforms develop and enforce content moderation policies, but his analysis centres on the speech implications rather than the identity implications. The distinction matters: losing your Facebook account is losing a platform. Losing your Google account is losing your identity.

### 7.2 The Labour Behind the Button

Sarah T. Roberts' *Behind the Screen* (2019) documents the human cost of content moderation – the workers who review violent and disturbing content for minimal pay. Her work reveals the labour structure beneath platform identity: humans decide who gets to exist digitally, under conditions that are themselves dehumanising. The system that deletes your identity is staffed by people whose own identities are ground down in the process.

### 7.3 The Ordinary Casualties

The four cases documented in Chapter 4 represent the gap in the literature. Mark, Dr. Buttfield-Addison, the Iranian developers, and the inactive account purge are not political de-platformings.

They are identity executions of ordinary people. The academic literature has not yet absorbed what this means at scale: that the power to delete an identity – not a post, not a profile, an identity – rests with companies that operate outside any democratic framework.

The evidence is thin not because the phenomenon is rare but because the victims are invisible. A father in San Francisco who loses his Google account does not write a journal article about it. He spends three weeks writing addresses on paper and two trips to the bank. The academic record of de-platforming is biased toward the famous because the famous have platforms from which to complain. The ordinary casualties disappear.

---

## Chapter 8: Self-Sovereign Identity – Why the Technical Solution Failed

### 8.1 The SSI Movement

The self-sovereign identity (SSI) movement (Allen, 2016; Preukschat & Reed, 2021) proposes decentralised identity systems where individuals control their own credentials without relying on central authorities. Christopher Allen's 2016 essay "The Path to Self-Sovereign Identity" outlined ten principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimisation, and protection. These principles are correct. They describe what identity should look like. They do not describe what identity does look like.

W3C's Decentralised Identifiers (DIDs) and Verifiable Credentials standards provide technical specifications for self-sovereign identity. The specifications are sound. They have been published, reviewed, and standardised. They define how a person can create a globally unique identifier controlled by their own cryptographic keys, and how credentials (age, citizenship, qualifications) can be issued, held, and verified without a central authority.

### 8.2 The Adoption Gap

SSI adoption remains negligible. The reason is structural, not technical: Google controls identity not because its technology is superior but because it controls the ecosystem. A cryptographic key that no service accepts is not an identity – it is a curiosity. The gap between SSI's technical viability and its practical adoption illustrates the difference between a protocol and a monopoly.

The SSI community has spent a decade building technically correct systems that nobody uses. The failure is instructive:

1. **Network effects protect incumbents.** "Sign in with Google" works on millions of websites. A DID works on zero websites that a normal person visits.
2. **Key management is hard.** Asking people to manage cryptographic keys is asking them to be their own bank. Most people do not want to be their own bank. They want to log in and see their photos.
3. **The chicken-and-egg problem.** No website supports DIDs because no users have DIDs. No users get DIDs because no websites support them.
4. **Blockchain baggage.** SSI became associated with cryptocurrency and blockchain, which carry reputational weight that repels mainstream adoption.

### 8.3 What SSI Got Right

SSI's core insight is correct: identity should be controlled by the individual, not by a corporation or a government. The ten principles are sound. The technical specifications work. The failure is not conceptual. It is strategic.

The alternative described in this thesis – physical attestation combined with client-side cryptographic derivation – learns from SSI's failure. It does not ask users to manage keys. It derives keys deterministically from inputs the user already knows (name, date of birth, secret words). It does not require website adoption. It generates a standard Ethereum address that works with any system that accepts Ethereum addresses. It does not depend on a blockchain for identity (only for optional voting and token operations). And it grounds digital identity in physical presence – something no purely digital system can do.

---

## Chapter 9: The Alternative – Physical Attestation and Sovereign Infrastructure

### 9.1 The Protocol

The alternative to corporate identity has been designed, built, and is described in detail in OMXUS Paper 20 ("Be In The Same Room At The Same Time"). The core protocol:

- 4 people stand in a room
- 60 minutes, same global window, 4 times per year
- BLE devices confirm co-presence
- Everyone signs off on the head count
- Your identity is verified by humans who can see you, not servers that track you

No Google account needed. No Apple device required. No Meta social graph analysed. No GitHub profile evaluated. No Microsoft login.

Just humans, confirming other humans exist, using physics instead of platforms.

### 9.2 What This Replaces

| Corporate Identity | Human Identity |
|---|---|
| Google decides you exist | Your neighbours confirm you exist |
| Apple permits you to use your device | You own your device |
| Meta holds your relationships hostage | Your relationships exist between you and other humans |
| GitHub owns your professional history | Your work speaks for itself |
| Microsoft controls your job access | Your identity is independent of your employer |
| Ban = digital death | Your body is your identity. Nobody can ban your body. |
| $1.037 trillion/year to maintain | Free |

### 9.3 Why Physical Attestation Succeeds Where SSI Failed

Physical attestation bypasses every failure mode of SSI:

1. **No network effect required.** You don't need websites to adopt your identity system. You need four people in a room.
2. **No key management.** Keys are derived from inputs you already know. Forget your key? Re-derive it from the same inputs.
3. **No chicken-and-egg.** The identity exists as soon as four people confirm each other. It doesn't need to be accepted by a website to be real.
4. **No blockchain baggage.** The attestation is a physical event. The cryptographic layer is invisible to the user.
5. **Sybil resistant.** You cannot fake physical presence. A bot cannot stand in a room. A fake account cannot make eye contact.

### 9.4 Why They Won't Like This

Every dollar these companies earn depends on being the identity layer. If identity moves to mutual human attestation:

- "Sign in with Google" becomes unnecessary – you already proved you're real
- Apple's walled garden loses its lock-in – your identity isn't tied to their devices
- Meta's social graph becomes optional – your relationships exist in the mesh, not on their servers
- GitHub's professional identity monopoly breaks – your contributions are signed by your identity, not your GitHub profile
- Microsoft's enterprise identity control evaporates – your employer no longer controls who you are

Combined revenue at risk: **$1.037 trillion per year.**

That's why this hasn't been built by them. Not because it's hard. Because it's worth a trillion dollars a year to make sure it isn't.

---

## Chapter 10: VexID – Implementation Architecture

### 10.1 Client-Side Identity Derivation

The OMXUS identity system, implemented in VexID, derives cryptographic identity entirely in the user's browser. No network request is required. No server sees the seed. The process:

1. **Inputs:** Name + date of birth + secret words (4+ words chosen by the user)
2. **Normalisation:** Inputs are normalised to prevent case/whitespace variations from producing different keys
3. **BIP-39 Seed Generation:** Normalised inputs are processed through PBKDF2-SHA512 (2048 rounds) to produce a 512-bit seed
4. **BIP-32 Key Derivation:** The seed is used to derive a hierarchical deterministic key using path `m/44'/60'/0'/0/0` (standard Ethereum derivation path)
5. **secp256k1 Keypair:** The derived key produces a secp256k1 private/public keypair
6. **Ethereum Address:** The public key is Keccak-256 hashed and truncated to produce a standard 20-byte Ethereum address

The same inputs always produce the same address. On any device. In any country. Offline. Forever.

### 10.2 Challenge-Response Authentication

When a user needs to prove their identity to a service (without revealing their seed):

1. Client sends their Ethereum address to the server
2. Server returns a random challenge string
3. Client signs the challenge with their private key (EIP-191)
4. Client sends the signature (v, r, s components) to the server
5. Server recovers the signing address from the signature using ecrecover
6. If recovered address matches claimed address, identity is confirmed

The server never sees the private key. The server never sees the seed phrase. The server never sees the name, date of birth, or secret words. The server only learns that the person who signed the challenge controls the private key corresponding to the claimed address. This is zero-knowledge identity verification.

### 10.3 Implementation Reality

This is not a whitepaper. The implementation exists:

- **core.js** (47KB): Full identity derivation – Keccak-256, BIP-39/32, secp256k1, address generation
- **omxus.py** (413 lines, zero dependencies): Pure Python reimplementation – identical output, verified
- **omxus-crypto.js**: Multi-backend secp256k1 wrapper (WebCrypto, noble-secp256k1)
- **fido2.js**: WebAuthn/FIDO2 for $29 hardware ring as second factor
- **attestation.js**: Device trust payload builder

The JavaScript and Python implementations produce identical keys and addresses from identical inputs. This has been verified. The identity is platform-independent.

### 10.4 What This Means for the Five Gates

With VexID:

- You do not need a Google account to prove you are real
- You do not need an Apple device to hold your identity
- You do not need a Meta profile to maintain your relationships
- You do not need a GitHub account to sign your code
- You do not need a Microsoft login to access your work

Your identity is derived from things you know. It lives in your head. No company can delete it. No server can lose it. No terms of service can revoke it.

---

## Chapter 11: Mesh Networking – You Are the Infrastructure

### 11.1 The Infrastructure Monopoly

The identity monopoly has a twin: the infrastructure monopoly. Even if you solve identity, you still need a network to communicate. That network is currently provided by ISPs – companies that charge monthly fees for access to infrastructure that your tax dollars often subsidised. In Australia,

the NBN (National Broadband Network) cost $51 billion of public money. Australians pay Telstra, Optus, and TPG for access to infrastructure they already paid for.

Mesh networking eliminates the ISP. Your device communicates directly with nearby devices using radio protocols that are already built into your phone:

- **Bluetooth Low Energy (BLE):** Range ~100m, low power, already in every phone
- **WiFi Direct:** Range ~200m, higher bandwidth, already in every phone
- **LoRa:** Range ~10km, low bandwidth, requires a $10 module

When enough devices participate, the mesh self-heals and self-routes. A message from your phone reaches any other phone in the mesh by hopping between intermediate devices. No tower. No cable. No ISP. No monthly bill.

### 11.2 The Connection to Identity

Mesh networking and sovereign identity are not separate projects. They are the same project. Corporate identity exists because corporate infrastructure exists. "Sign in with Google" works because Google controls the servers. If communication happens peer-to-peer, there is no server to sign in to. Identity becomes what it should be: a cryptographic proof that you are who you claim to be, verified by the people around you, transmitted through a network that you collectively own.

This is Goal 8: the internet costs nothing because you are the internet. The $29 ring in your pocket is both your identity token and your mesh node. When you walk into a room, the network gets stronger. When your neighbour's nan falls, the ring broadcasts to every device within 60 seconds. No call centre. No ambulance dispatch. No 14-minute wait. Your people come.

### 11.3 Implementation Status

The transport layer is built:

- **WireGuard tunnels** for encrypted point-to-point connections
- **Headscale** (self-hosted Tailscale) for mesh coordination
- **Yggdrasil** for IPv6 mesh with automatic LAN discovery
- **FRP** for CGNAT bypass

The human layer is built:

- **Hyperswarm DHT** for serverless device discovery
- **ntfy.sh** for self-hosted push notifications
- **Nostr bridge** using the same secp256k1 keys as VexID
- **WebRTC + Yjs** for live collaboration with offline-first CRDTs

The BLE mesh protocol for phones is 80% complete. The remaining 20% is contract calls for on-chain attestation.

---

## Chapter 12: The Permission We Gave

Here's the thing nobody wants to hear: they didn't take our identity. We gave it to them. One click at a time.

We clicked "Sign in with Google" because it was easier than remembering a password.

We bought iPhones because they were pretty.

We joined Facebook because our friends were there.

We used GitHub because everyone else did.

We logged into Office 365 because our boss told us to.

Each click was a vote. Not for a person – for a system. And the system we voted for is one where five companies in California decide whether 8 billion humans get to exist digitally.

We can un-vote.

Four people. One room. One hour. Four times a year. No California required.

---

## Chapter 13: Who Owns You? – The Kitchen-Table Version

*This chapter presents the thesis argument in language that requires no academic background. If you read nothing else, read this.*

---

Imagine your Google account disappeared tomorrow. Not deactivated – gone.

Your email – gone. Every account that uses "Sign in with Google" – locked. Your photos from the last decade – gone. Your calendar, your contacts, your documents – gone. Your two-factor authentication – gone, which means every other account protected by it is also gone. If you have an Android phone, it's a brick.

You didn't die. But try to prove you exist.

### The Five Companies That Own Your Identity

**Google** – 1.8 billion accounts. They have your email, your searches, your location history, your photos, your voice recordings, and your authentication to everything else. Revenue: $307 billion/year. From selling predictions about you.

**Apple** – 2.2 billion devices. They can remotely disable your phone, remove apps you paid for, block you from installing software they don't approve of, and revoke your purchases. Revenue: $383 billion/year. Including a 30% tax on every app.

**Meta** – 3.7 billion users. That's 46% of all humans. They hold your relationships, your messages, your community groups. In countries where WhatsApp is how people communicate, a Meta outage is a national emergency. Revenue: $135 billion/year. From your social graph.

**GitHub** – 100 million developers. Your code, your professional history, your portfolio. In 2019 they blocked developers in Iran, Syria, and Cuba. Not for anything they did – for where they were born. Owned by Microsoft.

**Microsoft** – 1.2 billion Office users. Your employer uses Microsoft. Microsoft controls your work email, documents, and login. Your job depends on your Microsoft account. Your rent depends on your job. Revenue: $212 billion/year.

Combined: **$1.037 trillion per year.** Funded by data you gave them for free.

### How It Happened

Nobody handed Google their identity. It happened one click at a time.

2004: Free email. You sign up. 2007: Pretty phone. You create an Apple ID. 2008: Your friends are on Facebook. You join. 2011: "Sign in with Google" appears. Easier than a new password. You click it. 2020: Pandemic. Everything's online. These accounts aren't convenience anymore – they're survival.

Each click was rational. The total is captivity.

### What They Know vs. What You Know

Google knows: every search you've made, every email you've sent, every place you've been, every purchase, every app, your face, your voice, your fingerprint, every website you've visited.

You know about Google: it has a colorful logo.

That's the deal you agreed to. Paragraph 47 of a document no human has ever finished reading.

### The Ban Button

There is no trial. No jury. No appeal with a guaranteed timeline. No public defender. No presumption of innocence.

There is a terms of service agreement and a button.

One person at one company presses it and you stop existing. Your email, your photos, your contacts, your authentication, your phone – gone. Not because you broke a law. Because you broke a rule written by a company you never voted for, in a document you never read, governed by a legal system in a country you may never have visited.

The US government needs a warrant to read your email. Google reads every email you send. You agreed to it. Paragraph 47.

### Why This Hasn't Been Fixed

Because fixing it costs them a trillion dollars a year.

Every dollar these companies earn depends on being the identity layer. "Sign in with Google" isn't a feature – it's a monopoly. If you could prove your identity without Google, you wouldn't need Google. If you didn't need Google, Google couldn't sell predictions about you. If Google couldn't sell predictions about you, there goes $307 billion.

Multiply by five companies. That's why.

It's not a conspiracy. It's just business. Your identity is their product. They're not going to help you take it back.

### The Fix

Four people stand in a room. Same hour, everywhere on Earth, four times a year. Your phones confirm you were there. Everyone signs off on the head count.

That's it. You're verified. No Google. No Apple. No Meta. No GitHub. No Microsoft.

Your neighbours confirm you exist. Not a server in California.

| Before | After |
|---|---|
| Google decides you exist | Your neighbours confirm you exist |
| Apple permits you to use your phone | You own your phone |
| Meta holds your friendships hostage | Your friendships are between you and your friends |
| One company bans you = digital death | Nobody can ban your body |
| $1.037 trillion/year to maintain | Free |

### The Part That Hurts

They didn't take your identity. You gave it to them.

One click at a time. Because it was easy. Because it was free. Because everyone else did.

And now five companies you never voted for, in a country most of you don't live in, get to decide whether you exist.

You can take it back. Same way you gave it away – one decision at a time. Starting with: stand in a room with three humans and say "I'm here."

No trillion-dollar company required. Just people.

---

The research version is in the chapters above. The trillion-dollar number is in the references. We're not telling you to delete anything. We're just asking: who presses the button?

---

## Chapter 14: Bill

Bill is 43 and lives in Geelong. He's a sparky – licensed electrician, 22 years in the trade. He's got a wife, two kids, a ute with 280,000 km on it, and a Google account he made in 2006 because his mate told him Gmail was better than Hotmail.

Bill doesn't think about Google. He uses it for email, for maps, for YouTube when he's eating lunch in the van. He's got Google Photos because that's where his phone puts them. He's got Google Authenticator because his bank told him to set it up. He's got "Sign in with Google" on his super fund, his insurance, his union portal, and the electrical licensing board.

Bill's 14-year-old son watches YouTube. One day the kid posts something in a comment section that triggers an automated moderation flag. Google's system links the comment to the family's shared account. The account gets suspended pending review. Not banned – suspended. "We'll get back to you."

Three weeks pass. During those three weeks:

- Bill can't access his email. His electrician's licence renewal notice was sent there. He misses the deadline.
- Bill can't access Google Authenticator. His bank requires it. He can't log in to pay his mortgage.

- Bill can't access Google Maps. He's been a sparky for 22 years in this city. He uses maps every day for new job sites. He writes addresses on paper for three weeks like it's 1998.
- Bill can't access his super fund portal because it uses "Sign in with Google." He was going to roll over a small account. The window closes.
- Bill can't access his photos. His mum is 71. She asked him to print the photos from last Christmas for her scrapbook. He can't.
- Bill's Android phone works, technically. But it nags him every four minutes to sign in. Half his apps won't open. It feels like driving a car with the engine light on permanent.

Bill calls Google. There is no phone number. There's a form. He fills it out. He gets an automated response that says "We'll review your case." He fills out another form. Same response.

Bill's wife asks him why he's in a bad mood. He doesn't know how to explain that a company in California – a company he's never met, never voted for, never signed a contract with that he actually read – has frozen his life because his son typed something stupid in a YouTube comment.

After 26 days, the account is restored. No explanation. No apology. No acknowledgement of the three weeks of disruption. Bill's electrician's licence renewal is now overdue. He has to pay a late fee and file paperwork to get it sorted. His bank eventually resets his 2FA, but it takes another week and two trips to the branch.

Bill ranked 47 candidates on a senate ballot the size of a tablecloth and none of them called him back. Nobody in parliament represents him. Nobody at Google knows his name. But both of them – the parliament and the company – get to decide how he lives.

Bill's not a radical. Bill's not political. Bill just wants to do his job, see his mates on Saturday, and not have a company he's never met control whether he can pay his mortgage.

Bill's story isn't about Google being evil. It's about what happens when your identity doesn't belong to you. Bill did nothing wrong. His kid did something dumb on the internet, like every 14-year-old since the internet was invented. And for 26 days, Bill couldn't function.

Three neighbours in a room. That's the alternative. Bill walks in, his mates vouch for him, his identity is confirmed by people who've known him since he was wiring houses at 21. Nobody in California required. Nobody can press a button and freeze his life.

That's not radical. That's just how it was before we gave it away.

---

## References

### Academic Sources

Allen, C. (2016). The path to self-sovereign identity. *Life With Alacrity* [blog]. http://www.lifewithalacrity.com/20 path-to-self-soverereign-identity.html

Couldry, N., & Mejias, U. A. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336–349. https://doi.org/10.1177/1527476418796632

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Halpern, O., & Mitchell, R. (2022). *The smartness mandate*. MIT Press.

Jhaver, S., Boylston, C., Yang, D., & Bruckman, A. (2021). Evaluating the effectiveness of deplatforming as a moderation strategy on Twitter. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–30.

Pasquinelli, M. (2023). *The eye of the master: A social history of artificial intelligence*. Verso.

Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning.

Roberts, S. T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press.

Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication*, 35(3), 213–229.

W3C. (2022). *Decentralized Identifiers (DIDs) v1.0*. W3C Recommendation. https://www.w3.org/TR/did-core/

W3C. (2022). *Verifiable Credentials Data Model v1.1*. W3C Recommendation. https://www.w3.org/TR/vc-data-model/

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

### De-Platforming Case Studies

Buttfield-Addison, P. (2025, December 13). 20 years of digital life, gone in an instant, thanks to Apple. *hey.paris*. https://hey.paris/posts/appleid/

Dillet, R. (2019, July 29). GitHub confirms it has blocked developers in Iran, Syria and Crimea. *TechCrunch*. https://techcrunch.com/2019/07/29/github-ban-sanctioned-countries/

Fung, B. (2022, August 21). A dad took photos of his naked toddler for the doctor. Google flagged him as a criminal. *The New York Times*. [Reported via multiple outlets including 9to5Google and Malwarebytes.]

Lyons, K. (2022, August 22). Google locked parent's account over medical photos of their child. *9to5Google*. https://9to5google.com/2022/08/22/google-locked-account-medical-photo-story/

NPR. (2023, December 2). Google starts deleting Gmail accounts that have been inactive for over two years. *NPR*. https://www.npr.org/2023/12/02/1216716083/google-starts-deleting-gmail-accounts-that-have-been-inactive-for-over-two-years

Wyden, O. (2025, December 13). Locked out: How a gift card purchase destroyed an Apple account. *AppleInsider*. https://appleinsider.com/articles/25/12/13/locked-out-how-a-gift-card-purchase-destroyed-an-apple-account

### Industry Reports and Data

Apple Inc. (2023). Apple reports first quarter results. *Apple Newsroom*. https://www.apple.com/newsroom/

BBC. (2021, October 5). Facebook outage: What went wrong and why did it take so long to fix? *BBC News*. https://www.bbc.com/news/technology-58886902

GitHub. (2019, July 29). GitHub and trade controls. *GitHub Blog*. https://github.blog/2019-07-12-github-and-trade-controls/

GitHub. (2023). Octoverse 2023: The state of open source. *GitHub*. https://github.blog/news-insights/octoverse/

IETF. (2012). *The OAuth 2.0 Authorization Framework*. RFC 6749. https://tools.ietf.org/html/rfc6749

Litmus. (2024). Email client market share. *Litmus Email Analytics*. https://www.litmus.com/email-client-market-share

Meta Platforms. (2024). Meta reports fourth quarter and full year 2023 results. *Meta Investor Relations*. https://investor.fb.com/

Microsoft. (2024). Microsoft fiscal year 2023 annual report. *Microsoft Investor Relations*. https://www.microsoft.com/en-us/investor/

OpenID Foundation. (2014). *OpenID Connect Core 1.0*. https://openid.net/specs/openid-connect-core-1_0.html

StatCounter. (2024). Mobile operating system market share worldwide. *StatCounter Global Stats*. https://gs.statcounter.com/os-market-share/mobile/worldwide

Statista. (2024). Number of Gmail users worldwide. *Statista*. https://www.statista.com/

### Technical Specifications

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

BIP-32: Hierarchical Deterministic Wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

BIP-39: Mnemonic code for generating deterministic keys. https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

EIP-191: Signed Data Standard. https://eips.ethereum.org/EIPS/eip-191

---

## Appendix A: Key Statistics

| Statistic | Value | Source | Year |
|---|---|---|---|
| Google accounts worldwide | 1.8 billion+ | Statista | 2024 |
| Android global market share | 71.8% | StatCounter | 2024 |
| Gmail email client market share | 29.7% | Litmus | 2024 |
| Active Apple devices | 2.2 billion | Apple | 2023 |
| iCloud users | 850 million+ | Apple | 2023 |
| Meta monthly active users (all platforms) | 3.74 billion | Meta | 2024 |
| GitHub users | 100 million+ | GitHub | 2023 |
| GitHub repositories | 330 million+ | GitHub | 2023 |
| Microsoft 365 users | 1.2 billion+ | Microsoft | 2024 |

| Statistic | Value | Source | Year |
|---|---|---|---|
| Azure AD daily authentications | 1.2 billion | Microsoft | 2024 |
| LinkedIn users | 1 billion | Microsoft | 2024 |
| Google revenue (2023) | $307 billion | Google | 2024 |
| Apple revenue (2023) | $383 billion | Apple | 2024 |
| Meta revenue (2023) | $135 billion | Meta | 2024 |
| Microsoft revenue (2023) | $212 billion | Microsoft | 2024 |
| Combined revenue | $1.037 trillion | Calculated | 2024 |
| Google Photos stored | 4 trillion+ | Google | 2023 |
| Windows desktop market share | 72% | StatCounter | 2024 |
| Facebook 2021 outage duration | 6 hours | BBC | 2021 |
| Google inactive account purge start | December 1, 2023 | NPR | 2023 |
| GitHub trade restriction countries | Iran, Syria, Crimea, Cuba, North Korea | TechCrunch | 2019 |
| Buttfield-Addison Apple ID tenure | ~25 years | hey.paris | 2025 |
| Mark (SF father) account lock | Permanent (police cleared, Google refused) | 9to5Google | 2022 |

---

## Appendix B: Cross-References to OMXUS Research Series

### Direct Dependencies

| Paper | Title | Relationship to This Thesis |
|---|---|---|
| **Paper 20** | Be In The Same Room At The Same Time | **Core dependency.** Defines the physical attestation protocol that replaces corporate identity. Four people, one room, one hour, four times a year. This thesis argues *why* corporate identity must be replaced; Paper 20 specifies *how*. |
| **Paper 07** | Trust-First Governance | Describes governance without corporate identity infrastructure. If identity is sovereign, governance can be sovereign. The trust model in Paper 07 depends on the identity model described here. |

### Parallel Arguments

| Paper | Title | Relationship to This Thesis |
|---|---|---|
| **Paper 09** | Grief to Design | Argues that tools should be designed from human need, not corporate convenience. The identity system described here is a grief-to-design product: it exists because corporate identity failed real people. |

| Paper | Title | Relationship to This Thesis |
|---|---|---|
| **Paper 12** | Bullshit Jobs | Examines how Microsoft's enterprise identity control perpetuates unnecessary work. Section 2.5 of this thesis (Microsoft: The Enterprise Identity) provides the identity infrastructure that Paper 12's work analysis sits on top of. |
| **Paper 14** | Swiss Direct Democracy / Voting | Cannot vote freely with corporate identity. If Google can delete your identity, Google can delete your vote. Paper 14 describes the voting mechanism; this thesis describes why that mechanism cannot run on corporate infrastructure. |
| **Paper 30** | The Smartness Trap | Extends the theoretical framework (Halpern & Mitchell, Couldry & Mejias) used in Chapters 5-6 of this thesis. |

### Infrastructure Papers

| Paper | Title | Relationship to This Thesis |
|---|---|---|
| **Paper 10** | (Transactions) | Free transactions require free identity. If identity is corporate, transactions are surveilled. |
| **Paper 13** | Community Emergency & Policing | The $29 ring (Goal 13) requires mesh networking (Chapter 11) and sovereign identity (Chapter 10). A community emergency response system cannot depend on a platform that goes down for six hours and takes hospitals with it. |

### Related Research Directories

| Directory | Relationship |
|---|---|
| `screens_attention_economy/` | Documents the attention extraction economy that identity lock-in enables. Section 4.4 of this thesis connects identity monopoly to attention monopoly. The same companies that control who you are control what you see. |
| `democratic_voting_mechanisms/` | Papers 08 (Quadratic Voting) and 14 (Swiss Direct Democracy) describe voting systems that require sovereign identity to function. Corporate identity makes sovereign voting impossible: if Google can delete your identity, it can delete your vote. |
| `sybil_resistance_physical_presence/` | The anti-Sybil mechanism for the physical attestation protocol. Explains why physical co-presence defeats fake accounts in ways that CAPTCHA, phone verification, and government ID cannot. |
| `ble_mesh_networking/` | Technical specification for the BLE mesh layer described in Chapter 11. The radio protocol that makes your phone a network node. |

| Directory | Relationship |
|---|---|
| `sovereign_ai_infrastructure/` | The same monopoly pattern applied to artificial intelligence. Five companies control identity; three companies control AI. The structural argument is identical. |

---

## Appendix C: Image Inventory

| File | Dimensions | Format | Description |
|---|---|---|---|
| `cover.jpg` | 1376x768 | JPEG | Dark dramatic scene with large illuminated letters G, F, A, A, M representing the five tech gatekeepers (Google, Facebook, Apple, Amazon, Microsoft). A sign in the centre reads "CAPTIVE IDENTITY VS SOVEREIGN IDENTITY." Background shows a digital constellation pattern behind the letters with storm clouds above. The framing suggests a gate or prison – the letters are the bars, the constellation is what's trapped inside. Note: uses the older GFAAM acronym rather than the thesis's final five (Google, Apple, Meta, GitHub, Microsoft). |
| `fingerprint_circuit_board.png` | 1920x1080 | PNG | Glowing blue fingerprint centred within a luminous ring, surrounded by circuit board traces radiating outward with bright nodes at connection points. Dark background. Represents the intersection of biological identity (the fingerprint, the thing that's yours) and digital infrastructure (the circuit board, the thing they built around it). The fingerprint is at the centre but the circuit board controls the pathways. |

---

*This document unifies Papers 22 and 23 of the OMXUS Research Series with the literature review, original analysis, implementation documentation, and cross-references. All content from the individual manuscripts is preserved. New material has been added in Chapters 10, 11, and the appendices.*

*The research version is in the chapters above. The trillion-dollar number is in the references. We're not telling you to delete anything. We're just asking: who presses the button?*