Abstract

Five corporations -- Google, Apple, Meta, GitHub, and Microsoft -- currently function as de facto identity authorities for the majority of the world's digital population. Disabling a Google account eliminates access to email, documents, photos, calendars, authentication tokens, and in many cases the ability to use an Android phone. Apple controls app distribution, payment identity, and device activation for over 2.2 billion devices. Meta owns the social graph of 3.7 billion people. GitHub gates access to the infrastructure of modern software. Microsoft controls enterprise identity for over 1.2 billion Office 365 users. None of these companies were elected. None were appointed. None were granted this authority by any democratic process. They assumed it because we authenticated with them, stored our data with them, and built our professional and social lives on their platforms. This paper examines how identity became privatized, what it costs, and why the alternative -- mutual physical attestation between humans -- requires no corporation at all.

Keywords: digital identity, platform dependency, identity sovereignty, corporate gatekeeping, de-platforming, authentication monopoly, data colonialism, surveillance capitalism, smartness mandate

1. Introduction

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.

---

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 license. 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.

---

3. How Identity Got Privatized

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 labor, platforms use convenience to extract behavioral 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 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.

---

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 behavior to companies that want to modify your behavior (Zuboff, 2019). Matteo Pasquinelli describes this as a "planetary business of surveillance and forecasting" (Pasquinelli, 2023, p. 12) -- the extraction of behavioral patterns at civilizational 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, monetized.

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 monetizing identity data that users provided for free.

---

5. The Alternative Already Exists

(Applebee & Combe, 2026, "*Be In The Same Room*") describes a system where identity verification requires no corporation:

- 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 analyzed. No GitHub profile evaluated. No Microsoft login.

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

5.1 What This Replaces

CORPORATE IDENTITY	HUMAN IDENTITY
Google decides you exist	Your neighbors 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.

5.2 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. Not because it's hard. Because it's worth a trillion dollars a year to make sure it isn't.

---

6. 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.

Series Context

This paper is part of the OMXUS Research Series.

The alternative to corporate identity -- four humans in a room confirming each other exist -- is laid out in full in (Applebee & Combe, 2026, "*Be In The Same Room*"). That protocol doesn't need Google. It doesn't need Apple. It needs a room and an hour. Everything in this paper builds toward the question (Applebee & Combe, 2026, "*Be In The Same Room*") answers: what does identity look like when no company owns it?

The work system examined here, where Microsoft controls your login and your login controls your livelihood, is the same system (Applebee & Combe, 2026, "*The Bullshit Jobs Phenomenon*") pulls apart. Bullshit jobs exist in part because the employer controls the infrastructure of personhood. You can't quit if quitting means losing your identity. (Applebee & Combe, 2026, "*Civic Proximity Response*") asks a different question -- what would we build if we started from grief instead of convenience? -- and reaches the same answer: the tools people need should not be owned by the people selling them.

None of this works if your vote passes through corporate infrastructure. (Applebee & Combe, 2026, "*Swiss Direct Democracy*") makes that case for voting. (Applebee & Combe, 2026, "*Cooperative Capitalism*") makes it for transactions. (Applebee & Combe, 2026, "*Wanted Attention for Unwanted Results*") makes it for communication -- community emergency response can't run through a platform that goes down for six hours and takes hospitals with it. Corporate identity is the lock that holds all of these systems in place. Physical co-presence is the key that opens every one of them.

(Applebee & Combe, 2026, "*The Smartness Trap*") takes the theoretical framework used here -- Halpern and Mitchell's "smartness mandate," Couldry and Mejias' data colonialism -- and extends it further. (Applebee & Combe, 2026, "*Trust-First Governance*") describes what governance looks like when trust replaces permission.

See `references/` *for full reference list.*