The New Design Congress

THE DIGITAL IDENTITY EVENT HORIZON

A NEW DESIGN CONGRESS RESEARCH REPORT
FIRST EDITION - AUGUST 2025

The New
Design Congress

Cade Diehm (New Design Congress)
Benjamin Royer (New Design Congress)

with contributions by
Roel Roscam Abbing (Independent Researcher)

Edited by
Rocío Armillas Tiseyra and Rose Regina Lawrence

Artwork by
Ignatius Gilfedder & Cade Diehm

With thanks to Esra'a Al Shafei, Dan Girshovich, Peter van Hardenberg, Matthew Canham, Meredith Whittaker, Matt Bailey, Caroline Sinders, John Marshall, Tian Tse, Eriol Fox, Teresa Zolnierkiewicz, Eleftherios Diakomichalis, Elio Qoshi, Laura Summers, Ilya Kreymer, Elys Day, Louis Center, Brent Bailey, Sandro Herbig, Dietrich Ayala, Danielle Brathwaite-Shirley, Allen "Gunner" Gunn, Aljoscha Meyer, Sammy Gwilym, Joe Hunting, Andrew Sempere, Chad Kohalyk, and Cent Hosen.

Read online:
https://newdesigncongress.org/en/report/2025/the-digital-identity-event-horizon

Table of Contents

Foreword: The Mask-Off Moment for Digital Identity

For more than four years, we've been researching the hidden fragility of digital societies, tracing how digital identity creates brittle systems that enable exploitation, exclusion, and social engineering. Drawing on eight global case studies, dozens of expert interviews, and hundreds of citations, this is our most significant research endeavour since NDC's founding at the turn of the decade.

It is also, without exaggeration, the most alarming body of work we have ever produced.If you work in digital identity, you may already be feeling a little defensive. That's a good thing, it means you're still reachable. While *The Digital Identity Event Horizon* is urgent and furious, this report is far from a condemnation. Rather, we publish as an appeal to those willing to confront the situation we collectively must grapple with. If you choose to continue down this trajectory after reading what follows, then yes, the condemnation is directed at you. And you will deserve it.

In this foreword, I want to explain why.

> *"There has been no fraud in 12 years. Estonia is the only country in the world where all IDs have the same legal value. This is a powerful incentive for use."*
>
> Helar Laasik
> Chief Expert, Estonian Police and Border Guard Board[1]

The quote above from 2014 was one of the first political statements we analysed at the start of this project. At the time, we approached it with a healthy and bemused scepticism; our hypothesis, that *digital identity creates brittle societies*, was shaped by our ongoing institutional work around social engineering, coercive design, and infrastructural failure. Still, we were not prepared for what we found: when we investigated Laasik's claim seriously, we were stunned by the sheer scale of its denial.

At the time Helar Laasik made this statement, an audit by Estonia's financial regulator uncovered extensive money laundering activities at Danske Bank's Estonian branch.[2] The

[1] Helar Laasik, quoted in Secure Identity Alliance, *Estonia Visit Report*, 14 June 2014, https://secureidentityalliance.org/publications-docman/public/11-14-06-02-sia-estonia-visit-report/file.

[2] Holger Roonemaa and Oliver Kund, "Newly Obtained Audit Report Details How Shady Clients from Around the World Moved Billions Through Estonia," *Organized Crime and Corruption Reporting Project*, 12 March 2021, https://www.occrp.org/en/investigation/newly-obtained-audit-report-details-how-shady-clients-from-around-

audit revealed that billions of dollars in suspicious transactions were processed through the bank, involving clients from Russia, Azerbaijan, and Ukraine. The auditors identified numerous instances where the bank failed to question dubious transactions, accepted inadequate documentation, and ignored red flags, effectively enabling large-scale financial fraud.[3]

Meanwhile, in October 2014, an exploitable vulnerability[4] was introduced into the Estonian ID card system. It went undetected for three years, quietly compromising the cryptographic integrity of over 750,000 active cards. And it occurred at the exact moment the system was being touted as bulletproof.[5]

Today, even despite this contradiction, the legend of the Estonian eID success persists as a global poster-child for the digital identity movement. But in 2023 alone, Estonia's citizens endured an ongoing 25% year-on-year growth in fraud cases[6], with losses of €21.5 million to cyber[7] and payment fraud.[8] These figures are just a fraction of what we document in our forthcoming Estonian case study. Together, this quote and the reality of Estonia's situation is a visceral encapsulation of the threat that faces us: digital identity as a structural fraud-permissive ecosystem misrepresented as secure, precise, progressive, and, perhaps most egregiously, empowering.

We begin here because it sets the tone for what's to come. This quote, and the reality it concealed, foreshadowed the structural permissiveness we now document at every level of the global digital identity movement. From Laasik's claim as our starting point, and over the course of our research, we have watched the optimism of digital identity's proponents be erased by opportunists, vandals, and vulgar, second-rate power in real time. Now, as we prepare to publish, the polite façade of digital identity has shattered; every principal threat model we outlined in 2024 can now be observed in operation; some at pilot scale, others nationwide.

the-world-moved-billions-through-estonia.

[3] European Parliament, *Report on Financial Crimes, Tax Evasion and Tax Avoidance [TAX3], A8-0170/2019*, 26 March 2019, https://www.europarl.europa.eu/doceo/document/A-8-2019-0170_EN.html.

[4] Matúš Nemec, Marek Sys, Petr Švenda, Dušan Klinec and Vashek Matyáš, "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security [CCS '17]*, 2017, https://crocs.fi.muni.cz/public/papers/rsa_ccs17.

[5] Bruce Schneier, "Security Flaw in Estonian National ID Card," *Schneier on Security* [blog], 5 September 2017, https://www.schneier.com/blog/archives/2017/09/security_flaw_i.html.

[6] ERR News, "Crime in Estonia Rises 4 % on Year, Fraud up 25 %," *ERR.ee*, 8 January 2024, https://news.err.ee/1609522354/crime-in-estonia-rises-4-on-year-fraud-up-25.

[7] E-Estonia Briefing Centre, "2023: Estonia and the Advanced Cybersecurity Threats," *e-Estonia*, 28 December 2023, https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats.

[8] Eesti Pank, "Estonian Payment Forum Searched for Ways of Preventing Payment Fraud," 16 January 2025, https://www.eestipank.ee/en/press/estonian-payment-forum-searched-ways-preventing-payment-fraud-16012025.

In other words, all of the threats described in this report have materialised. *Every single one.*

In my 12-year career, I have never, ever seen anything like it.

Under the reinstalled Trump administration, the United States is conducting an unprecedented programme[9] of mass detention and deportation.[10] Digital identity is central to this scheme, weaponised across borders,[11] communities,[12] and institutions.[13] These are only a few of the many avenues this hyper-violent regime exploits. The daily stories are horrific and enraging. It is clear this punitive, discriminatory, malevolent operation is lubricated by digital identity.

Meanwhile, Trump's newly minted Department of Government Efficiency (DOGE)[14] has executed a hostile takeover of the U.S. civil-identity stack.[15] In late June 2025, the agency unveiled a searchable national citizenship database built with DHS and Palantir.[16] Civil-liberties groups describe it as "a surveillance nightmare," yet it now sits live behind voter-roll checks, benefit eligibility and deportation orders.

For over two decades, the proponents of digital identity, including Estonia and its global supporters, insisted that accountability was its safeguard. What DOGE reveals is just how meaningless that guardrail always was. The billionaire Musk and his acolytes walked in the front door at the exact moment the U.S. administration began rounding up non-citizens and openly threatening to send its own citizens to overseas black sites. No one stopped him.[17]

[9] Michael Waldman, "Trump's Mass Deportation Plans," *Brennan Center for Justice*, 19 November 2024, https://www.brennancenter.org/our-work/analysis-opinion/trumps-mass-deportation-plans.

[10] Juliana Kim, "Here Are the Immigration Provisions in Trump's Megabill," *NPR*, 3 July 2025, https://www.npr.org/2025/07/03/1252663607/trump-immigration-megabill-provisions.

[11] U.S. Customs and Border Protection, "CBP Completes Simplified Arrival Expansion at All U.S. Airports," 29 May 2024, https://www.cbp.gov/newsroom/national-media-release/cbp-completes-simplified-arrival-expansion-all-us-airports.

[12] Fatima Hussein, "IRS Acting Commissioner Is Resigning over Deal to Send Immigrants' Tax Data to ICE, AP Sources Say," *Associated Press*, 2025, https://apnews.com/article/d2ac6f7ac0a1f60e907cd3b52d0db34d.

[13] The Economic Times, "Kicked Out Without Warning: SEVIS Terminations Leave Hundreds of International Students in Legal Chaos," 2025, https://economictimes.indiatimes.com/nri/study/kicked-out-without-warning-sevis-terminations-leave-hundreds-of-international-students-in-legal-chaos/articleshow/120518548.cms.

[14] Johana Bhuiyan, "Trump Officials Create Searchable National Citizenship Database," *The Guardian*, 30 June 2025, https://www.theguardian.com/us-news/2025/jun/30/trump-citizenship-database-doge.

[15] Aaron Gregg, "Privacy Under Siege: DOGE's One Big, Beautiful Database," *Brookings Institution* [blog], 26 June 2025, https://www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/.

[16] Robert Weissman and Lisa Gilbert, "Public Citizen Co-Presidents Request to Join DOGE," *Common Dreams* [press release], 4 July 2025, https://www.commondreams.org/newswire/public-citizen-co-presidents-request-to-join-doge-2670807823.

[17] Adele Peters, "What Will It Take to Stop Elon Musk and DOGE?" *Fast Company*, 5 February 2025, https://www.fastcompany.com/91272862/what-will-it-take-to-stop-elon-musk-and-doge.

The US does not act alone. Israel's IDF employs digital identities crafted from SIM card metadata and arbitrary digital footprints to execute indiscriminate drone strikes, stripping away human complexity in favour of algorithmic assassination.[18] These tactics are built on the one-user-one-device assumption that dominates Western software and security design, a premise already unstable in the Global North,[19] and entirely delusional when exported to occupied or precarious regions. For Palestinians, as for much of the world, smartphones are shared objects passed between siblings, between lovers, lent to neighbours, shared within households. This collective relationship to technology is the norm.[20]

In the face of communal data intimacy, the IDF's targeting infrastructure becomes not only inaccurate, but unfathomably cruel: a fire-and-forget strategy of serialised murder masquerading as precision. It is a system of violence built on pseudo-scientific operational laziness, in which the intimate logistics of survival are flattened into unaccountable to-kill spreadsheets and .CSVs.

In Ukraine, digital identities are repurposed as existential weapons in the conflict with Russia.[21] The country is paralysed, its ability to govern is fractured by the ongoing war, which includes the targeted sabotage of its digitised infrastructure. Core identity systems, once touted as enablers of governance, now serve as liabilities that are compromised and weaponised.

Kyiv's digitisation has come at great cost. Across the wider conflict, leaked identity records are dumped online by hostile actors, forming the substrate of a multi-domain asymmetrical war. Personal records are weaponised[22] to psychologically destabilise civilians,[23] to impersonate, to mislead, and to fracture trust in every domain of daily life.[24] In occupied territories, the strategy reaches a brutal coda: seized databases are mined to identify and

[18] Human Rights Watch, "Gaza: Israeli Military's Digital Tools Risk Civilian Harm," 10 September 2024, https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm.

[19] Amit Kumar Sikder et al., "KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home," *arXiv* preprint arXiv:1911.10186 [2019], https://arxiv.org/abs/1911.10186.

[20] Palestinian Central Bureau of Statistics, "PCBS & the Ministry of Communications and Information Technology," 2022, https://www.pcbs.gov.ps/post.aspx?ItemID=4510&lang=en.

[21] George Ingram and Priya Vora, "Ukraine: Digital Resilience in a Time of War," *Brookings Institution*, 15 January 2024, https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/.

[22] Nataliya Khandusyenko, "Selling Personal Data of Ukrainians: Criminal Group Exposed in Sumy Region," *dev.ua*, 4 February 2025, https://dev.ua/en/news/prodavaly-personalni-dani-ukraintsiv-na-sumshchyni-rozkryto-zlochynnu-hrupu-1738679055.

[23] "How Telegram Is Used for Psychological Warfare against Ukraine," *Uttryck Magazine*, 27 February 2025, https://www.uttryckmagazine.com/2025/02/27/telegram-war-fuels-itself/.

[24] Nick Corbishley, "Remember Ukraine's 'Diia' Digital Governance System? Russian Hackers Brought It Down in December, and It Is Still Partly Down," *NickCorbishley.com* [blog], 31 January 2025, https://nickcorbishley.com/2025/01/31/remember-ukraines-diia-digital-governance-system-russian-hackers-brought-it-down-in-december-and-it-is-still-partly-down/.

assassinate civilians based on demographics, affiliations, or past activity, converting the entire premise of civil registry into a tool for literal algorithmic execution.[25] [26]

From the examples listed, to the brutal information-fuelled war in Sudan,[27] to India's multi-decade struggle with digitised election infrastructure,[28] to the suicides of Australia's most vulnerable welfare recipients under former Prime Minister Scott Morrison's Robodebt scheme,[29] the failures of digital identity are like an oil slick over a shared human condition that is poisoned by screaming, financially incentivised bots; crude assemblages designed to endlessly extract and earn for their operators, an information network saturated with noise. I am not talking about disinformation. It doesn't matter what they say. What matters is that they exist to trick users that they are real people. What matters is that they exist at all, and that systems that were meant to connect us now nakedly *"lean in"* – to borrow a term from one of this situation's chief architects, Sheryl Sandberg – to the opportunity to facilitate total information decline.

Against the backdrop of such naked, vicious, identity-enabled atrocities, the United Nations has announced a global plan to eliminate boarding passes and airport check-ins, replacing them with facial recognition and "digital journey passes" stored on travellers' phones.[30] The press frames it as a leap forward in convenience and security. But there is no possible reconciliation between this vision and the world as it exists. It is simply not possible to hold the reality of 2025 alongside promises like these. Whether journalist, politician, or technologist, *to perform such a denial is to participate in future atrocity*.

~

If you come away from what I've described here wholly indignant of my condemnation of any of my examples, I'm sorry to say, *you are being fooled.* No matter your perspective on any of these examples, I'm not here to debate your side. The sides don't matter. Here's what

[25] Bathsheba Nell Crocker to Michelle Bachelet, letter, United States Mission to the United Nations, 20 February 2022, reproduced in *The Washington Post*, https://www.washingtonpost.com/context/read-u-s-letter-to-the-u-n-alleging-russia-is-planning-human-rights-abuses-in-ukraine/93a8d6a1-5b44-4ae8-89e5-cd5d328dd150/.

[26] Human Rights Watch, "Ukraine: Torture, Disappearances in Occupied South," 22 July 2022, https://www.hrw.org/news/2022/07/22/ukraine-torture-disappearances-occupied-south.

[27] Maram Mahdi and Kyle Hiebert, "Sudan's Conflict Is Being Fuelled by a Digital Propaganda War," *Middle East Eye*, 6 June 2023, https://www.middleeasteye.net/opinion/sudan-civil-war-digital-propaganda-campaigns-fuelling.

[28] Andy Mukherjee, "India's Voting Machines Are Raising Too Many Questions," *Bloomberg Opinion*, 11 April 2024, https://www.bloomberg.com/opinion/articles/2024-04-11/india-election-too-many-questions-loom-over-voting-machines.

[29] Patrick Marlborough, "How Robodebt Killed Vulnerable People Like Me," *VICE*, 9 December 2020, https://www.vice.com/en/article/how-centrelink-robodebt-killed-vulnerable-people-like-me-suicide/.

[30] Nawaf Al Zadjali, "Digital Travel Credentials: A New Standard for Identity Management" *[presentation, ICAO Facilitation Panel [FALP/13] Meeting*, Montréal, 22-26 April 2024], https://www.icao.int/Meetings/FAL2024/Documents/Presentation_Nawaf%20Al%20Zadjali.pdf.

does: our digitised society was designed and built in a childlike *“End of History”*[31] bet, an unquestioning belief in an ideological fiction popularised after the Cold War, and on an assumption that liberal capitalist democracy had triumphed as the final form of human government. This is a system built on *hopium*, a fingers-crossed wish for stability, integration, and progress. Digital identity systems were architected inside this delusion, as if geopolitics, collapse, or technological misuse were things of the past. This is colossally wrong. The architecture of digital identity is indifferent to your ideology. It does not care which ’side’ you think you are on. I cannot stress this enough: you are vulnerable, and this will be used against you.

Today’s status quo allows for the design and implementation of dangerous digital identity systems without consequence. This is indefensible, and if you’re reading this report, you likely agree. We reject a future dictated by digital tyranny or the ugliness of electronic chaos. This report and the case studies that follow are designed to force a reckoning; do not look away. Digest these findings. Print them. Translate them. Leak them upstream. This is the end of the *End of History*, and we are living through volumes unfolding all at once. The choices you make today are not just your own. They are the conditions others will inherit.

If you do one thing after reading *The Digital Identity Event Horizon*, let it be this: put this report in front of someone who still believes in digital identity as it exists today, so that we may start to recognise and respond to the threat together. But even if we fail, this work exists so that, regardless of what atrocities await us, those who enabled the infrastructure of harm cannot one day claim ignorance.

The most tragic outcome would be for the very architects of digital identity to one day shrug and say, *“We had no idea.”* This report exists so they never can. ✳

Cade Diehm
August 2025

[31] ‘*The End of History*’ is a geopolitical state argued by Francis Fukuyama, where the end of the Cold War signalled the final triumph of liberal democracy and market capitalism as the ultimate form of human government. His thesis suggested that ideological evolution had ended, a belief that deeply influenced 1990s political and technological culture-and critically shaped the naïve assumptions underlying digital infrastructure development.
Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992), https://www.simonandschuster.com/books/The-End-of-History-and-the-Last-Man/Francis-Fukuyama/9780743284554.

Executive Summary

Digital identity is a foundational paradigm of contemporary digital systems, and is perhaps the most important component for its role in representing actors and entities in complex socio-technical systems. Driven by the accelerating importance of this paradigm in all facets of modern life, the roles, capability, control and custodianship of digital identity are hotly contested.

Digital identity is also the primary vector for attacking and disrupting digital systems. For example, in the five-year lead up to 2017, US companies paid an estimated $1.6 billion as a result of social engineering attacks. In the same time period, the probability of success for a social engineering attack jumped by 15%, to a staggering success rate of three out of four.[32]

As the 2020s reveals itself to be a decade of fragmentation and international conflicts coupled with emergent biometric, blockchain, and machine learning technologies, digital identity reveals itself as a major battleground that facilitates economic and information warfare. Hyper-connected societies rely on digital identity to govern, communicate, and transact, and we are only just beginning to grapple with the wide-spread weaponisation of the representation of the digital self.

This research is an ambitious compilation of digital identity, its historical influences, and implementations in the first half of the 2020s. It uses threat modelling, qualitative research interviews and direct collaboration with key partners to understand the socio-technical vulnerabilities of identity systems, and features specific case studies focused on incumbent or emergent identity paradigms.

This research finds that current models of digital identity are brittle to social engineering attacks, and that the digital identity discipline has not successfully grappled with issues of over-identification, abuse of digital identity, or the second- and third-order effects of different identity systems. Research findings show a trend towards an incomplete reckoning of digital identity, threatened by over-financialisation, and the continued reliance on a '*I authenticate, therefore I am*' model of digital representation. The outcomes of the current state of affairs, documented through participant testimonies and existing literature, are extreme and often-times violent.

However, the need for trustworthy digital identity is more pressing than ever, and opportunities exist to develop new norms around the role of identity and what it represents,

[32] Cynthia Lopez Olson, 'Social Engineering Attacks by the Numbers: Prevalence, Costs, & Impact', *Dataflog*, 15 February 2019, https://dataflog.com/read/social-engineering-attacks-numbers-cost/.

the introduction of legislation around custodianship and weaponisation of identity, advocacy for strong accountability for digital identity providers, and the systemic encouragement of compartmentalisation of identity markers, such that their abuse or breach is not catastrophic. ✳

Problem Statement I: Digital identity creates brittle societies

"We hypostatize information into objects. Rearrangement of objects is change in the content of the information; the message has changed. This is a language which we have lost the ability to read. We ourselves are a part of this language; changes in us are changes in the content of the information. We ourselves are information-rich; information enters us, is processed and is then projected outward once more, now in an altered form. We are not aware that we are doing this, that in fact this is all we are doing."[33]

~

When individuals, organisations, and other entities are represented within a digital system, the design and emulation of this representation is called a *digital identity*. Digital identity is a multifaceted socio-technical[34] construct that facilitates online interactions and transactions, serving as a virtual representation of an entity. It plays a critical role in enabling a wide range of activities in the digital environment, from personal communication to professional engagements, and is subject to concerns related to privacy, security, resilience and authenticity. **Despite the development of sophisticated cryptographic systems and security practices, and widespread multi-decade efforts to deploy these defence mechanisms, digital identity remains the weakest link in systems design.** What does it take to assemble a digital identity? What do different implementations of digital identity share?

Key Points

› Digital identity represents people, institutions, devices, and other entities.

› Common to all digital identity are seven properties: *Serialisation*, *Custodianship*, *Presentation*, *Authentication*, *Authorisation*, *Assetisation*, *and Mutability.*

› Each of the seven properties of a digital identity have systemic flaws.

› Because identity is central to all networks, the flaws in the seven properties become opportunities for compromise by an adversarial actor within any digital system.

› Attacks that leverage digital identity are often non-technical in nature.

[33] Philip K. Dick, *VALIS,* [Boston: Houghton Mifflin, 1981].

[34] Socio-technical refers to the 'emergent interplay between tools and behaviours of users,' and is especially useful in emerging digital security practice. See also: Matt Goerzen, Elizabeth Anne Watkins, and Gabrielle Lim, 'Entanglements and Exploits: Sociotechnical Security as an Analytic Framework', *9th USENIX Workshop on Free and Open Communications on the Internet*, 13 August 2019, https://www.semanticscholar.org/paper/Entanglements-and-Exploits%3A-Sociotechnical-Security-Goerzen-Watkins/d84cd734911393b07fc9cd6a12da1f36564994f.

The roots of digital identity trace back to the 19th century. One significant early application of digital identity was its use in the 1890 United States Census,[35] representing an early systemic embedding of the punch card system as a tool for governance and state sense-making. This would develop into the modern computing field in the following century. As societies have digitised and computerised, the use and influence of digital identities has expanded dramatically, with different context-sensitive implementations of digital identity touching nearly all parts of modern life.

Anticipating and examining the effects of digital identity on governance, commercial activity, and the social interactions of digitised societies requires a more concrete definition of the *first principle*[36] of digital identity. Despite the universal and multi-faceted deployment of digital identity in modern life, there is no agreed-to standard definition of what exactly encompasses digital identity.[37] This ambiguity stems from the broad range of datasets used to define and structure a digital identity system, the equally-broad objective and application of the identity within a wider digital system, and the competing interests held by bodies that define and deploy digital identity systems.

Depending on the intended use case, internal or external constraints, legislative requirements, or other factors, digital identities are derived from what data they are designed to hold. Through the act of serialisation, in which aspects of a person are converted into a data set, a digital identity takes form once it is capable of storing one or more entity-representing data sets for later lookup. Common data that make up a digital identity system include:

› **Unique identifiers** specific to the identity system, including usernames or other system-assigned addresses;

› **Personal identifying information** within the context of the identity (attributes), such as an individual’s full name, address, gender, date of birth, etc;

› **User curated data**, such as a profile photo, account name, or self-assigned categorisations;

[35] Steven Lubar, ‘“Do Not Fold, Spindle or Mutilate”: A Cultural History of the Punch Card’, *The Journal of American Culture* 15, no. 4 (1992), https://onlinelibrary.wiley.com/doi/10.1111/j.1542-734X.1992.1504_43.x

[36] A first principle is a fundamental, foundational concept or assumption that serves as the bedrock for a system’s design, operation, and understanding. A first principle is not derived from other principles or assumptions but stands as an axiom. It coalesces from a complex set of political, material and ideological constraints, and guides the development and function of any cybernetic system that supports digital identity.

[37] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee, ‘The Identity Crisis Security, Privacy and Usability Issues in Identity Management’, arXiv, 2 January 2011, https://arxiv.org/abs/1101.0427.

- Passwords, passkeys, or other **security primitives**, such as cryptographic key pairs;

- **User-generated behavioural or transactional data**, such as network activity, financial records, location histories, or other unique information logs;

- **Online or offline social graphs**, including self-declared, observed, or inferred real-world or digital relationships, and other associations;

- **Data assigned by a third party, such as classification** by an identity vendor, social credit scores, credit histories, or criminal records;

- **Network association**, such as domain instance[38] or choice of protocol;

- **Additional non-human data**, such as MAC addresses, or other hardware information when identities represent devices, or corporate branding and other legal information where identities represent organisations and entities;

Each of these data types have a profound effect on the shape and potential application of a digital identity in areas of trust, privacy, capability, accuracy, governance, social dynamics, power, integrity, and colonialism.[39] Across the discipline of the digital identity first principle, the assembly and structure of this data is both highly contextualised within its own boundaries, at the same time diffuse and amorphous in the aggregate.

The digital identity first principle is often well understood within its immediate application, but not regulated or standardised[40] due to the wider complexity of the multitudes of implementations, diverse motivations of differing implementations, and influence of marketing and/or lobbying. For example, the IP address of a residential customer of an Internet Service Provider can either represent a digital identity or a *data-point* in a digital identity. The discrepancy between these two perspectives has significant consequences: the treatment of IP addresses as a legally sound representation of 'user-centric'[41] digital identity was a core strategy of corporate litigation against private citizens during the file-

[38] A domain instance refers to a top level domain associated with a user account, particularly in federated networks. For example, in the case of the mastodon account *@cade@newdesigncongress.org*, the domain instance is *newdesigncongress.org*.

[39] Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3-26.

[40] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee, 'The Identity Crisis Security, Privacy and Usability Issues in Identity Management', arXiv, 2 January 2011, https://arxiv.org/abs/1101.0427.

[41] For a definition of this term, see the Problem Statement III chapter.

sharing lawsuits of the 2010s.[42] So long as a cluster of data points is used to identify an entity of some kind, it can be classified as an example of a digital identity.

The application of digital identity is equally broad and varied, as digital identities are deployed in the pursuit of institutional, legislative, or ideological objectives. The objectives can be radical: privacy-focused projects such as Signal[43] or the Tor Project[44] deploy a kind of digital identity designed to defend against the de-anonymisation of users, while simultaneously ensuring that users are able to identify each other reliably (user-to-user, in the case of Signal) or attempting to offer a degree of reliability when looking up the identity of Onion-based web services (user-to-device, in the case of Tor), or to provide cryptographic verification using device-based identities, a practice common to both projects.

At the other extreme, immigration and border control objectives rely on detailed digital identities derived from a mix of data – criminal records, observational profiles, social histories, and other data points held by state or private actors. As an individual enters or exits a country, border agents use e-passports and biometric scans as a kind of namespace lookup,[45] first comparing the real-world individual to their documentation, and then retrieving additional data designed to assess and record the transiting individual's history and character.

Between the examples of network privacy and border control, the application of digital identity has countless forms: self-curated profiles on social media platforms, digital currency wallets, advertising profiles, credit histories, networks of trust, social credit scores, virtual reality or VTuber avatars, digital banking profiles, government-to-citizen services, computer operating systems, and text-based chat systems are just a handful of examples of products and services that depend upon the application of digital identities. The objectives of these examples determine not just what is contained within an identity, but also what the identity is capable of representing, and the validity of the claims of what is represented. Social media platforms such as Facebook, TikTok, or Bluesky, and developer services such as GitHub offer identity variations to represent organisations and companies alongside individual users, and sometimes allow users to use their identity to authenticate and associate themselves with an organisation. Internet of Things (IoT) or device-first systems

[42] 'RIAA v. The People: Five Years Later', *Electronic Frontier Foundation*, 30 September 2008, https://www.eff.org/wp/riaa-v-people-five-years-later.

[43] Signal is a cryptographically secure open-source messaging service.

[44] The Tor Project is primarily responsible for maintaining software for the Tor anonymity network, a decentralised anti-censorship web browsing network.

[45] A name[space] lookup is the act in which a supplied name, when encountered in a program, is associated with the declaration that introduced it.

use identities to represent and authenticate machines – be it during interactions with other machines, or with users.

'Chester the otter,' a VTuber character by streamer Kris Yim. VTubers, or Virtual YouTubers, are livestreamers who perform using virtual avatars puppeteered by motion capture hardware and software.

The range of potential definitions and configuration of a digital identity model, combined with the multitudes of potential applications of these models plays a significant role in the inability of the technology and policy communities to communicate and build consensus around the design and use of this critical concept. As members of the ID2020 Web of Trust workshop asserted in their earlier 2011 paper *Identity Crisis: Clearer Identity through Correlation*.

> *"When we think about "identity" in terms of "who we are", we get caught up in the consequences and ramifications of policy and privacy and human rights. These are important debates, but they often slip into abstractions, miscommunication, and political disagreements that undermine our efforts to build functioning identity systems. On the other hand, when we think about "identity" as a mere collection of attributes or identifiers, we ignore and sometimes dismiss the deeper meanings others interpret in the word.*"[46]

~

In examining digital identity over the course of this research, we have identified a set of common properties that we propose as a universal definition of digital identity for the purposes of the case studies, landscape review, and qualitative interviews contained in this research. **This is a multi-faceted, multi-perspective working definition for the first principle of digital identity that includes seven core properties**:

[46] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee, 'The Identity Crisis Security, Privacy and Usability Issues in Identity Management', arXiv, 2 January 2011, https://arxiv.org/abs/1101.0427.

1. **Serialisation**, in which part of an individual is read and converted into a digital form by a software or hardware sensory apparatus, and defined at the discretion of a systems designer;

2. **Custodianship**, in which the serialised self from which the identity is derived is stored and maintained in some form, be it via software automation or via manual means by the user[47] or a third party;[48]

3. **Presentation**, where the serialised data is reassembled and made legible to machines or humans through an interface of some kind;

4. **Authentication**, where the digital identity becomes a central mechanism in which an individual invokes some form of cryptography and/or relational trust to gain access to digital or real-world resources, services, opportunities, or is granted movement in a place;[49]

5. **Authorisation**, where the authentication and presentation layers of a digital identity act as a vessel for an individual that allows gatekeepers to give and maintain access to a system or resource;

6. **Assetisation**, where the digital identity is employed as the support for a wider financial speculation goal and/or other commercial ventures, and;

7. **Mutability**, where the designers of a digital identity determine whether the system will accept additional serialisations, and under what context such updates may occur.

Despite popular concepts of digital identity as tied to user self-expression or data-politics, the expression or representation of self is not the intent of the digital identity first principle. Instead, the overarching goal shared by all implementations of digital identity is that of the broader intent of cybernetics: to govern a population in aggregate. This is accomplished by standardising the properties of entities and actors as they appear within the digital system, eliminating edge cases where possible, and designing socio-technical touch points within the system that allow for the management of these subjects. Such an array of techniques

[47] Local first storage includes devices and services that opt to store user data on said user's local device, rather than a remote or centralised location, such as biometric data stored in Apple's Secure Enclave or a user's Steam game library. See also: Martin Kleppmann et al., 'Local-First Software: You Own Your Data, in Spite of the Cloud', in *Proceedings of the 2019 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software* [SPLASH '19: 2019 ACM SIGPLAN International Conference on Systems, Programming, Languages, and Applications: Software for Humanity, Athens Greece: ACM, 2019], https://gwern.net/doc/cs/algorithm/2019-kleppmann.pdf.

[48] For example, an IT department responsible for maintaining the user identities and data of a company.

[49] See for example the National Institute of Standards and Technology's approach to identity and authentication.

obeys a diffuse rationality in the act of *governementality*[50], a concept that is inseparable from the material and systemic tension points of society. The term governing here is broadly agnostic, applying equally to digital identity that serves to manage users on a Discord[51] server, to assign and disperse essential provisions to a population in crisis, or anything in between.

At the same time, the digital identity first principle is an individualistic paradigm. Although identities often represent companies, organisations, devices, or other non-human actors, these implementations are nevertheless derived from a Libertarian-inspired *one user one identity*[52] design popularised by technology advocates in the 2000s.[53] Aside from a few tightly controlled exceptions, non-individual identities become temporarily individual, or retain an individual identity developed over time. In an example of the former, users will frequently express themselves as an individual through the group identity, such as employees including their initials on messages posted from corporate social media accounts. For the latter, a device identity in an anonymous cryptocurrency system becomes an individual identity as it is subjected to forensic on-chain analysis and profiling over time.

All digital identities are *simulacra,*[54] in the sense that the processes of capture and reproduction of the identity are inherently flattening and imitative. The representation of self held within a digital identity is modified by the system and the hardware apparatus that supports the system itself. Pressing the organic world into silicon for the purposes of assembling a sort of diorama representation is achieved through standardisation and serialisation.

Even at the smallest scales, digital systems are fraught with compounding complexity, not just within their own design, but in the design of systems that support them — network topographies, sensor capabilities, storage considerations, etc. The same is true for the reassembly and presentation of the identity at a later stage. Entropy, edge cases, and nuance create significant challenges for the conceptualisation and operation of digital systems, and

[50] For Michel Foucault, governementality refers to the rationality of the act of governing, a practice he locates during the long birth of the liberal Nation State.

[51] Discord is a gaming-focused group chat platform where servers are administrated and moderated by users. The platform is notable for its advanced moderation tools relative to its competitors.

[52] Raphael Banda and Jackson Phiri, 'Challenges of Identity Management Systems and Mechanisms: A Review of Mobile Identity' [*ICICT 2018*, Lusaka, 2019], https://www.researchgate.net/publication/331952305_Challenges_of_Identity_Management_Systems_and_Mechanisms_A_Review_of_Mobile_Identity.

[53] Shun-Ling Chen, 'What's in a Name - Facebook's Real Name Policy and User Privacy', *SSRN Electronic Journal*, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3332188.

[54] The simulacrum is, for Jean Baudrillard, the end result of the process by which the sign discards any relationship with what it is supposed to represent or signify: a copy of a copy of reality, with no original, where signs simply call upon other signs. See also: Jean Baudrillard, *Simulacres et Simulation* [Paris: Éditions Galilée, 1981].

offline sources for digital identity are rich in all three. To reduce complexity and the tools used in the conversion contributes to tremendous data loss. As the Hong Kong philosopher Yuk Hui writes, *"Generally speaking, technological diversity is disappearing and becoming homogenized due to cybernetic hegemony. Technological development throughout the world now consists of nothing more than a vast process of "translation": exactly as with linguistic translation, we seek equivalences between different cultures for each element of the system – but that never really works."*[55]

Finally, all digital identities are eventually *human readable*. Regardless of the humanity of the intended counterparty (or lack of), all digital identity can and will eventually take a human readable form. This human legibility can be inherent to the system for which the digital identity was designed, such as a user profile interface in a social media platform, or a human-readable email address. Legibility can also be derived from the digital identity and its interactions within a digital system by a third party, for example the forensic analysis of a cryptocurrency wallet address and its social graph.

To assess a digital identity, one might consider the legibility of each of the core six seven properties of a digital identity: serialisation, custodianship, presentation, authentication, authorisation, assetisation, and mutability. These properties together form a model that interfaces with the real world. It is through this tactile and quasi-*Para-Real*[56] context that the strengths, flaws, risks, and opportunities are often considered. **Questions of universal access, digital literacy, disability, colonialism, privacy, security, discrimination, and other issues driven by digital identity are at their most visceral: in the inter-facing layer between the electronic world and those who gaze into it. It is precisely the complexity and intensity of this surface that encourages the deeper entrenchment of the flawed first principles of the electronic self.** ✳

[55] Michaël Crevoisier, 'Yuk Hui : « Produire des technologies alternatives »', *BALLAST*, 9 July 2020, https://www.revue-ballast.fr/yuk-hui-produire-des-technologies-alternatives/.

[56] Cade Diehm, 'The Para-Real: A Manifesto', *New Design Congress*, 10 December 2022, https://newdesigncongress.org/en/pub/the-para-real-manifesto/ .

Problem Statement II: The digital identity landscape is paralysed by misunderstanding and misuse

In Hong-Kong, a finance worker joins a video call–one of dozens they attend every week. This is not a routine call however: the meeting's agenda is a request to transfer HK$200 million. Familiar faces appear on-screen, their voices filling the headphones. In the flattened reality of this digital interaction, reassured by colleagues and superiors, the employee finalises the transfer details and wires the money.

None of those people were real. The money disappears.[57]

~

As you read this, the world has entered an era where no recorded voice or face can be trusted. Amongst the many system shocks the 2020s will be remembered for, **this is a tectonic shift that shatters how we cultivate social trust, especially in digital societies. Entrenched governance structures**, agitated by sudden paradigm changes, **have led us to this digital identity event horizon**; A pure science (non-)fiction timeline of crimes, made possible by the most intimate impersonations, stretches as far as the eye can doom-scroll. More recently, the rise of AI social engineering attacks highlights the pressing need for more technological solutions enforcing more robust authentication. How can this depressing state of affair, where no single attribute of a person can escape the reach of bad actors, be brought to an end?

Key Points

- › Digital identity has historical origins in a 'Cartesian rationalism' approach to self representation–"*I think, therefore I am*" becomes "*I authenticate, therefore I am.*"
- › Because digital identity is assembled from identity markers, these representations are incomplete and often contradictory.
- › When combined with external forces, this method for self-representation has profound consequences.
- › Digital identity is culturally and institutionally ingrained, and responding to its weaknesses represents a formidable systemic challenge.

Perhaps a more important question is, *how did we get here*? As trust in identity crumbles, the entire digital identity field is left incoherent. Lost to the mainstream digital identity discourse is a consistent definition of the very subject of the debates. Instead stands fledgling, market-driven governance cultivated by a cohort of self-selected experts–NGOs,

[57] Heather Chen and Kathleen Magramo, 'Finance Worker Pays out $25 Million after Video Call with Deepfake "Chief Financial Officer"', *CNN*, 4 February 2024, https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html .

politicians, technologists, executives and private consultants—all agitating for discrete interests and the 'common good.' Contradictory and competitive conceptualisations of the self lead to decisions made for entire populations, often with unexpected consequences.

Identity is everywhere, and as a result it is nowhere. **This fatal ambiguity arises from *Cartesian identity*—'I think, therefore I am'— an incomplete rationalist reckoning of the digital self that leaves actors of the field incapable to discern its shortcomings.** The digital identity landscape remains blind-sided by outcomes stemming from the limits of technical solutions derived from the Cartesian identity. Furthermore, it produces an attack surface that originates from *functioning* systems of identification.

~

In the previous chapter, we define the first problem statement of this research: that digital identity's first principle is ill-defined, untested, and brittle. Combined with the shaky convictions of triumphant post-Cold War liberalism,[58] and the tendency of this political philosophy to confuse ontology with ownership (being with having),[59] identity morphs from the output of an act of identification to the property of a person. The profound contradictions produced by this conceptual chasm reverberate when applied to systems of governance at scale.

The promises made by proponents of both past and emerging digital identity systems are varied and contradictory. Common to all is the claim that this digital identity will usher a new age of sovereignty, a digital equivalent of *just one more lane will fix traffic on this highway*. Here, digital identity is a rational tool, deployed both to know the self and to recognise the other. These opinions on **recognition** and **authentication** rely on deeply rooted claims to an individual's human rights and economic autonomy[60] where, puzzlingly, "one cannot have an absolute right over their body."[61] When presented as a cornerstone of governance, entire communities subjected to centuries of western colonial and post-colonial

[58] Liberalism here in the sense of the broader political philosophy and economy, which most sections of conservatism, socialism, social-democracy, etc. have embraced.

[59] Sara González, 'Pierre Crétois, Philosopher: "We Cannot Pretend to Be Absolute Masters of Things,"' *EL PAÍS English*, 21 July 2023, https://english.elpais.com/society/2023-07-21/pierre-cretois-philosopher-we-cannot-pretend-to-be-absolute-masters-of-things.html.

[60] "Digital Inclusion: A Human Right to Have an Identity," Thales Group, 2 February 2021, https://www.thalesgroup.com/en/dis/government/magazine/digital-inclusion-human-right-have-identity.

[61] Ananthakrishnan G, 'In Supreme Court, Centre Admits Aadhaar Data Leak, Critics Cite "Civil Liberties"', *The Indian Express*, 4 May 2017, https://indianexpress.com/article/india/govt-admits-aadhaar-data-leak-critics-cite-civil-liberties-4639819/.

exactions are expected to materialise the infrastructures of a western-modelled civic society—an expectation without reflection.[62]

When promoted as infrastructure policy, proponents claim that the new efficiencies and optimisations set free by digital identity will generate "a new frontier in value creation for individuals and institutions around the world."[63] Deep-seated ideological and logistical issues of old 'paper-based' bureaucratic registration systems will be solved. Consultants and ex-government officials, with a resume of shock therapy, austerity, and underfunding[64], will finally bring to heel "slow and cumbersome government services."[65] And in the disintegration of peace-time, these systems become pattern-of-life indicators, building target-able identities from scratch for optimised drone strikes.[66]

Such moral and material flexibility strikes at the heart of digital identity. The fatal ambiguity of such a benighted and chaotic definition of the digital self ensures that a desirable future cannot be achieved. A discipline that blends together commercial trust, human rights, and targeted assassinations under the same epithet offers only nihilism as its telos. So long as this status quo remains, digital identity, with its self-appointed grandiose remit, faces us as a weapon, not as an aspiration.

In 2000, Rogers Brubacker and Frederick Cooper summarised the identity crisis that had, by the time they published, already been unfolding for more than fifty years:

> *"The notion of identification was pried from its original, specifically psychoanalytic context [...]*
>
> *[The] term identity proved highly resonant in the 1960s, diffusing quickly across disciplinary and national boundaries, establishing itself in the journalistic as well as the academic lexicon, and permeating the language of social and political practice as well as that of social and political analysis. In the American context, the prevalent individualist ethos and idiom gave a particular salience and resonance to identity concerns,*

[62] Andrew Sever, 'Council Post: Digital Identity In Developing Countries: What Lessons Can Be Learned?', *Forbes*, accessed 12 April 2023, https://www.forbes.com/sites/forbestechcouncil/2023/04/12/digital-identity-in-developing-countries-what-lessons-can-be-learned/.

[63] Deepa Mahajan, Owen Sperling, and Olivia White, "Digital ID: The Opportunities and the Risks,", *McKinsey & Company*, 19 August 2019, https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks.

[64] Daniel Trilling, *Bloody Nasty People: The Rise of Britain's Far Right* (London: Verso, 2013).

[65] Kirsty Innes, Jeegar Kakkad, and Ryan Wain, "The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity", *Tony Blair Institute for Global Change*, 15 June 2023, https://www.institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.

[66] Grégoire Chamayou, *A Theory of the Drone,* trans. Janet Lloyd (London: Verso, 1 May 2015).

> *particularly in the contexts of the 1950s thematization of the mass society problem and the 1960s generational rebellion [...]*
>
> *The proliferation of identitarian claim-making was facilitated by the comparative institutional weakness of leftist politics in the United States and by the concomitant weakness of class-based idioms of social and political analysis."*[67]

The identitarian endeavour cannot be separated from the long era of technocratic solutionism unleashed in the wake of cybernetics.[68] Positioned as a humanist (and later human-centred) medium to pacify social conflicts, identity evolved into both a societal first principle and a theoretical fetish, a value-laden shorthand to self that could resolve a series of social antagonisms.[69] Today, 'cardinal' identities, or reference points for each person. are fast becoming the alpha and omega of any registration process. They seek to embody a natural right, property, and possession of any represented human. In a perverse inversion of this value system, life-threatening consequences looms over those falling short of its representational schemes.[70] At its extreme of confusion between *being* and *having*, such identities are dubbed *wallets*, whence the currency of all social interactions must flow.

Following the UN 2016 Sustainable Development Goal indicators and the World Bank ID4D initiative, digital identity designers began to advocate for a serialisation of cardinal identities. These include projects that allow users to split one's identity across multiple contexts,[71] or that advocate for context-sensitive, compartmentalised identities linked to one verifiable person,[72] as well as "self-sovereign" endeavours.[73] While their technical implementations may diverge, all these initiatives agree with the same basic identitarian premises, investing in identity's near-identical ontological power[74] and epistemic value.[75]

[67] Rogers Brubaker and Frederick Cooper Reviewed work[s]:, 'Beyond "Identity"', *Theory and Society* 29, no. 1 [2000]: 1-47, http://www.jstor.org/stable/3108478.

[68] Benjamin Royer, 'The Imperial Sensorium', *New Design Congress*, 21 June 2022, https://newdesigncongress.org/en/pub/the-imperial-sensorium.

[69] Inscribed on the UN Legal Identity Agenda: https://unstats.un.org/legal-identity-agenda/publications/.

[70] The Wire Staff, "Of 42 'Hunger-Related' Deaths Since 2017, 25 'Linked to Aadhaar Issues'," *The Wire*, 21 September 2018, https://thewire.in/rights/of-42-hunger-related-deaths-since-2017-25-linked-to-aadhaar-issues.

[71] OAuth is an open standard for integrating access and authentication across different websites and user accounts.

[72] Keybase is a digital security start-up that pairs PGP key security with social trust and verification by using 'proofs' on social media to determine identity authenticity.

[73] 'Generative Identity - beyond Self-Sovereignty', Philip Sheldrake, 2 September 2019, https://philipsheldrake.com/2019/09/generative-identity-beyond-self-sovereignty/ .

[74] As R. Brubacker & F. Cooper have noted, one must wonder why the same word is employed to described a fragmented partial or incomplete self, multiple partial selves, and multiple complete selves. The philosophical and psychological implications are even more bewildering.

[75] Alexandra Giannopoulou, 'Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity', *Digital Society* 2, no. 2 [2023], https://pubmed.ncbi.nlm.nih.gov/37200582/.

There exists already concrete consequences to the conceptual confusion engendered by the dangerously out-of-control reach of digital identity, and any system that relies upon this compromised first principle. In 2010, journalist and author Cory Doctorow documented the theft of his Twitter password via a phishing link sent to his DMs.[76] In 2024, he was successfully targeted *again* by another social engineering fraud, despite 14 years of allegedly more sophisticated digital security infrastructure and his own increased awareness to this threat.[77] Doctorow's anecdotal example points at a serious reality: with billions lost in conventional phishing techniques, what hope do we have to fight this future?

Emergent digital identity paradigms look beyond the password, into unique personal identifiers (such as biometrics) as authentication and presentation components. Keys derived from unique biological features or individual behaviours offer a compelling defence against a seemingly unstoppable wave of social engineering attacks. However what is clear by now is: if vulnerable passwords and passcodes remain the mainstay of digital identity theft, biometrics are subject, to rapid weaponisation[78], and thus to become new cardinal attack vectors.[79]

Offensive technologies are in active development, harvesting the rough materials for impersonation at a mass-scale aided by the multiplication of biometric sensors unleashed by consumer tech, for example smart speaker microphones, face-id cameras, and newly-introduced iris scans.[80] Fraudsters are not the only parties interested in such a rabid deployment of official, biometric-backed data-points.[81] This reality coexists with massive systemic failures such as the 2021 hack of the Argentinian Registro Nacional de las Personas, which saw the digital identities of the country's entire population stolen and sold

[76] Corey Doctorow, 'Persistence Pays Parasites', *Locus Magazine*, 6 May 2010, https://locusmag.com/2010/05/cory-doctorow-persistence-pays-parasites/.

[77] Corey Doctorow, 'How I Got Scammed', *Pluralistic*, 14 March 2024, https://pluralistic.net/2024/02/05/cyber-dunning-kruger/.

[78] Mathew J. Schwartz, 'Banking Trojan Harvests Facial Biometrics for AI Deepfakes', *Data Breach Today*, 15 February 2024, https://www.databreachtoday.com/banking-trojan-harvests-facial-biometrics-for-ai-deepfakes-a-24370.

[79] Emma Roth, 'X Wants Permission to Start Collecting Your Biometric Data and Employment History', *The Verge*, 31 August 2023, https://www.theverge.com/2023/8/31/23853618/x-privacy-policy-update-biometrics-job-history.

[80] Apple, Inc 'About Optic ID Advanced Technology', 2 February 2024, https://support.apple.com/en-us/HT214051.

[81] "When Bodies Become Data: Biometric Technologies and Free Expression." ARTICLE 19, 2021, https://www.article19.org/biometric-technologies-privacy-data-free-expression/.

piecemeal on the dark net,[82] the leak of Adhaar card-holders' personal information,[83] and the large scale theft of Okta's customer support's data.[84]

What drives this arms race? The answer is simple. **The assetisation of digital identity, combined with the flaws of the Cartesian identity, accrues tremendous value because all data-points in a digitised society are deemed credible enough to become a support for digital identity**. Patient records, credit scores, transactions, social media whereabouts, moods, citizenship, and ownership claims. What used to be considered mere *records* become *partial-identities*, and while initially carefully defined as such, end up quickly misused as full-fledged identity projects.

For instance, USAID, the avowed "tip of the spear" of the US soft power apparatus,[85] draws a distinction between *instrumental* approaches, where identity stems from a specific institutional need (such as patient records or driving licenses), and *foundational* ones, where the foundations for a comprehensive identity project are put in place.[86] Yet, USAID subsumed these two categories under the grand project of digital identity, with the first seen as a useful and potential stepping stone for the second. The two become inextricably linked, a cybernetic Möbius strip of conceptualisation, serialisation, and expansion. The world has already witnessed the tragic consequences of such cavalier conceptualisations, combined at scale with misplaced beliefs in soft-power management.[87]

Similarly, the Future of Identity in the Information Society (FIDIS), a "multidisciplinary endeavour of 24 leading institutions from research, government, and industry", which included IBM and Microsoft, took great pain in their 2009 proceedings to define the Global System for Mobile Communications (GSM) network as the medium for partial identities, whereby *"different sets of attributes (partial identities) are needed in different situations – and they can be made available due to the relative strength of the SIM [Subscriber*

[82] Catalin Cimpanu, 'Hacker Steals Government ID Database for Argentina's Entire Population', *The Record*, 18 October 2021, https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population.

[83] Ananthakrishnan G, 'In Supreme Court, Centre Admits Aadhaar Data Leak, Critics Cite "Civil Liberties"', *The Indian Express*, 4 May 2017, https://indianexpress.com/article/india/govt-admits-aadhaar-data-leak-critics-cite-civil-liberties-4639819/.

[84] Graham Starr, 'Okta Says Hackers Stole Data for All Customer Support Users', *Bloomberg*, 29 November 2023, https://www.bloomberg.com/news/articles/2023-11-29/okta-says-hackers-stole-data-for-all-customer-support-users.

[85] Margaret Seymour, 'Measuring Soft Power', *Foreign Policy Research Institute*, 14 December 2020, https://www.fpri.org/article/2020/12/measuring-soft-power/.

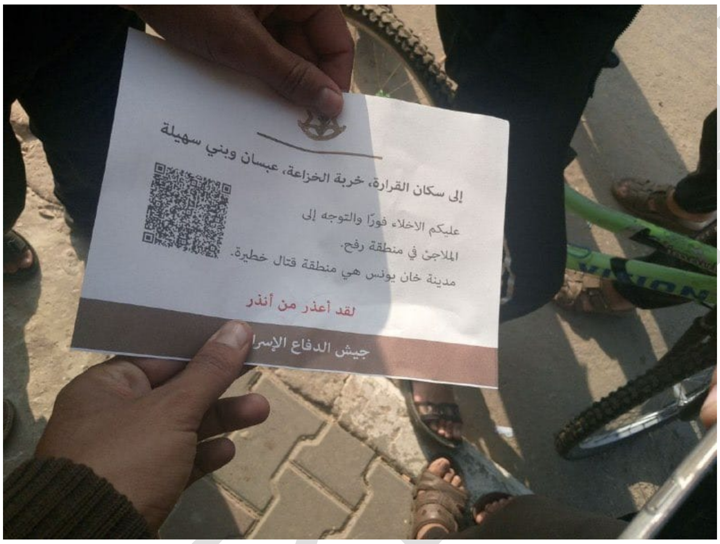
[86] 'Identity in a Digital Age: Infrastructure for Inclusive Development,' USAID, undated, https://www.simprints.com/wp-content/uploads/2024/07/Identity-in-a-Digital-Age.pdf

[87] Kai Rannenberg, ed., *The Future of Identity in the Information Society: Challenges and Opportunities* (Berlin Heidelberg: Springer, 2009).

Identity/Identification Module] card as a security token.'[88] Yet quickly, a self-contained *set of attributes* can be discussed as *identity per se*:

> *"The SIM concept, together with the supporting GSM infrastructure, provides both identity information and security for accessing voice services, data services, or context based services, such as LBS [Location-Based Services].'*[89]

The conflation of multiple unrelated attributes into an identity shorthand should not be seen as mere conceptual slip of the tongue or semantic shorthand, but a blurring of lines endemic to the digital identity discourse/practice. When considered alongside the use of IP addresses as legal evidence in dragnet intellectual property enforcement,[90] the GSM example reveals itself as a topological space where illegitimate reconfigurations of power manifest.



إلى سكان القرارة، خربة الخزاعة، عبسان وبني سهيلة

عليكم الاخلاء فورًا والتوجه إلى
الملاجئ في منطقة رفح.
مدينة خان يونس هي منطقة قتال خطيرة.

لقد أعذر من أنذر

جيش الدفاع الإسرا

Figure: Photo of the QR code used by IDF forces to advise Gazans of safe evacuation zones during airstrikes.[91]

Other cases are even more egregious. The Israeli Defence Forces (IDF) have long developed the practice of dropping leaflets in Gaza featuring QR codes leading Palestinians to a web page with a geolocation service, in order to 'help' the population avoid active combat zones and bombings. Worse than the widely reported failures of this "service",[92] is the perspective of the generation of "GSM identity information" tied to the well-established practice of

[88] Ibid.

[89] Ibid.

[90] Cade Diehm, 'This Is Fine: Optimism & Emergency in the P2P Network', *New Design Congress*, 16 July 2020, https://newdesigncongress.org/en/pub/this-is-fine.

[91] Aurora Intel [@AuroraIntel], "Found one without the code covered.," *X.com*, 1 December 2023, https://twitter.com/AuroraIntel/status/1730493340683030600.

[92] Steve Hendrix, Miriam Berger, and Hazem Balousha, 'Israel Touts Civilian Warning System, but for Gazans, Nowhere Is Safe', *Washington Post*, 7 January 2024, https://www.washingtonpost.com/world/2023/12/06/israel-gaza-civilians-protection/.

360-degree profile databases[93] and drone strikes[94] through "SIM card data, the interception of phone calls, and graphs of social networks."[95]

~

In a white paper produced as part of the 2016 Rebooting Web of Trust II workshop, Joe Andrieu *et al.* contested 'the appropriateness of focusing on "identity" as a property of a thing (or person), rather than as a phenomenon that emerges between an observer and a subject," noting that "using the word "identity" as a concrete, ownable, controllable asset obfuscates more than it communicates.' Within this seemingly semantic challenge lurks a deeply operational core:

> *"[...] any notion of identity is not particularly useful without the existence of a person or entity performing identification."*[96]

What's at stake here is the common denominator that connects it all—the million-dollar Hong Kong fraud, the social media password worm, the IDF bombing-shelter-as-a-service leaflet, and the biometrics deepfake mass-harvest[97]—as a single, uninterrupted contour of the digital identity event horizon. By eliding this core operation at the heart of identification, and instead focusing on a rhetoric of value-laden identity, the digital identity landscape has been unable to grapple with a key site of power and knowledge relations that has been weaponised over and over again.[98]

To describe the dire state of digital identity is not to condemn the discipline indiscriminately. The field is aware of the issues of surveillance, context collapse, and identity theft.[99] All these can however be assuaged by externalising the threats, or by defining a system as faulty or compromised. What the digital identity discipline is yet to fully address is the idea that a locus of power opens when identification performs *as*

[93] Srinivas Kodali, 'The Dangers of NATGRID and the Proliferation of 360-Degree Profile Databases', *The Wire*, 1 May 2023, https://thewire.in/tech/natgrid-and-360-degree-profile-databases-dangers/.

[94] Yuval Abraham, '"A Mass Assassination Factory": Inside Israel's Calculated Bombing of Gaza', *+972 Magazine*, 30 November 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/.

[95] Grégoire Chamayou, *A Theory of the Drone*, trans. Janet Lloyd (London: Verso, 1 May 2015).

[96] That can however always be potentially challenged and undermined, and this is addressed later in the report.

[97] Mathew J. Schwartz, 'Banking Trojan Harvests Facial Biometrics for AI Deepfakes', *Data Breach Today*, 15 February 2024, https://www.databreachtoday.com/banking-trojan-harvests-facial-biometrics-for-ai-deepfakes-a-24370.

[98] These issues are often acknowledged as abstractions without real-life use-cases or mostly as technical problems to be solved. If they are ever concretely addressed, the solutions often focus on commercial transactions. If the risks of political downfalls for users are ever mentioned, they occur in non-liberal democracies. The case of the French government creating terrorist records out of the identity of climate activists, or the UK Metropolitan Police abusing women through police officers with fake personas appear to us somehow very prescient.

[99] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (London: Penguin Classics, 2020).

expected, a systemic example of *weaponised design* as one party unilaterally assesses and gives permission. In what Michel Foucault describes as "micro-physics of power,"[100] domination and subjugation do not flow from institutions (or platforms, or databases, or even rogue nations) but rather within the mechanisms articulating social relations and giving them weight, serving as "weapons, relays, communication routes and supports for the power and knowledge relations that invest human bodies and subjugate them by turning them into objects of knowledge."[101] This complex social dynamic, that saturates all acts of registration and recognition, does not simply evaporate by claiming self-sovereignty through blockchain ledgers,[102] device enclaves[103], or zero-knowledge proof.[104]

The easy transition from human-centred value to financial value, permeating digital identity, only multiplies the potency of this power imbalance. In *Immigration Control and Fraud in Southern Africa*, Andrew MacDonald documents the lucrative operations, and the bodily harm, that can spawn out of registration systems. As the nascent South African State geared itself towards preserving its white population's dominance, it targeted the flow of Indian migrants with a complex system of certificates, testimonies, biometrics (fingerprinting), and other official documents, while claiming for itself the kind patriarchal values of imperial liberalism. The creation of a fraud incentive market helmed by bureaucrats and the heads of Indian trading families had unthinkably horrific consequences:

> *"The certificates gradually gained in monetary value. [Brokerage] houses became more sophisticated, where once they might merely have acted as exchange marketplaces, they diversified into the altering and endorsement of certificates (the going rate was about £5 per document). With a certificate came some rudimentary coaching in what to expect from South African immigration officials. [...] Some migrants arrived with multiple certificates as a form of insurance against theft; in some extreme cases impersonation required self-mutilation so that bodily scars might tally.*
>
> *As this economy grew more complex, so did the potential for profit."*[105]

[100] Ibid.

[101] Margie Cheesman, 'Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity', *Geopolitics* 27, no. 1 (1 January 2022): 134–59, doi:10.1080/14650045.2020.1823836.

[102] 'Breaking Encryption Myths', Internet Society, accessed 6 May 2024, https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/.

[103] Zach Whittaker, 'For $15,000, GrayKey Promises to Crack IPhone Passcodes for Police', *ZDNET*, accessed 19 March 2018, https://www.zdnet.com/article/graykey-box-promises-to-unlock-iphones-for-police/.

[104] See also: examples on how zero-knowledge is not a silver bullet in complex socio-political contexts.

[105] A. MacDonald, Immigration Control and Fraud in Southern Africa. One could raise the objection that this is the example of a system of identification that was gamed, with unexpected effects. However, the system worked as intended, or as best as it can be expected to work, given the conditions and the driving forces

These are the concrete outcomes that the digital identity discipline must reckon with as fundamental incentives and rewards baked into the material conditions that bear witness to the birth of digital systems. The avowed digital identity horizon is one where most – if not all – social interactions end up mediated by series of discrete, “partial” identifications.[106] Through precarious conceptualisations of identity, and its concretion into the design of digital systems, these identifications retain the full performative power of the cardinal identity they refer to.[107] In this *fallacy of identity composition*, the incentive to attack these small and diffuse partial identifications simply become too tantalizing. Our Hong Kong fraudsters simply had to imitate faces and voices: it netted them more than USD$25 million.

~

The digitised society clearly needs a way to represent the self. Social groups do require forms of mutual, inter-personal recognition that are often mediated through schemes of registration. And yet, the crises made possible by digital identity touch on every aspect of life. By 2024, hundreds of billions are lost through fraud,[108] an catastrophic economic loss achieved through the weaponised design of digital identity.[109] Digital identity has revealed itself to be a major attack surface in the two of the most scrutinised conflagrations of recent years: Ukraine and Gaza. The doxxing of Russian soldiers and spies’ personal information,[110] and the identification of Palestinian civilians[111] as well as warfare-based pattern-matching terrorist profiles,[112] reveal the extent to which

behind its creation: imperial liberalism, the closure of the colonial expansion of capitalism, and patriarchal white supremacism.

[106] FIDIS’ proceedings are particularly rich in dystopian case-studies of future applications.

[107] For how performativity influences registration, see T. Herzog, *Naming, Identifying and Authorizing Movement in Early Modern Spain and Spanish America*: “Rather than constituting the person as the bearer of certain rights and duties, [identity documents and registries] indicated he may be thus. Rather than operating a transformation [making someone worthy of a certain treatment by the act of registering him or her], they recognized the validity of a change in status that had transpired beforehand, in fact sanctioning what oral negotiations had already consecrated. More often than not, rather than representing ‘reality’, registries gave proof of attempts by authorities […] to control reality, attempts that were usually rejected […]. [Written] registries always coexisted with an oral knowledge that either opposed or converged with them. How these two different registers coexisted [and perhaps coexist today] is a story we still need to explore.”

[108] Dashveenjit Kaur, ‘Identity Theft Is Costing the British £4bn a Year’, *TechHQ*, 16 August 2022, https://techhq.com/2022/08/identity-theft-is-costing-the-british-4bn-a-year/.

[109] Anonymous, ‘Digital Identity in the US Is Broken’, *Bitcoin Policy Institute*, 2 February 2024, https://www.btcpolicy.org/articles/digital-identity-in-the-us-is-broken.

[110] Matt Burgess, ‘Russia Is Leaking Data Like a Sieve’, *Wired*, 13 April 2022, https://www.wired.com/story/russia-ukraine-data/.

[111] Patrick Kingsley and Ronen Bergman, ‘Tracking Cellphone Data by Neighborhood, Israel Gauges Gaza Evacuation’, *The New York Times*, 16 October 2023, https://www.nytimes.com/2023/10/16/world/middleeast/gaza-invasion-israel-cellphone-data.html.

[112] Bianca Baggiarini, ‘Israel’s AI Can Produce 100 Bombing Targets a Day in Gaza. Is This the Future of War?’, *The Conversation*, 8 December 2023, https://theconversation.com/israels-ai-can-produce-100-bombing-targets-a-day-in-gaza-is-this-the-future-of-war-219302.

identifying information, combined with cynical probability-based scoring systems, do not simply oil the cogs of credit and trust, but also of retaliation and massacre.

Far from these tragedies, one Friday night in your future, a loved one calls you unexpectedly. Their voice can be heard begging you to transfer your life savings to save them from peril.

They never called you. Your money is never seen again, and your bank, citing your biometric authentication of the transfer, refuses to refund your money.

With this scenario becoming a daily reality, the total collapse in the trust of the digital self is already here. ✳

Problem Statement III: Digital identity is amorphous and does not conform to conceptual models

Conceptualisation and governance are not the only aspects shaping the use and outcomes of digital identity systems. The topologies of digital identity, and their very observation, are additional dimensions that affect these socio-political structures. Existing research into digital identity management systems describe four such topological models: **"siloed," "centralised", "federated", and "user-centric."** These models can be used to trace how topologies enable specific relationships between users, identity providers, and service providers. **The models of digital identity offer methods for identifying deterministic points of control, risk, custodianship, and opportunity within any specific identity system. Each configuration has specific strengths and vulnerabilities, as well as contrasting implications for complexity, economic sustainability, and sovereignty.** To understand digital identity at a macro level is to evaluate the implementation of historical digital identity systems, or the potential of emergent or proposed new systems through these models. This contributes to an important materialist analysis of the entanglement of rhetoric and reality within complex systems at scale.

Key Points

- There are four models (or 'spheres') of digital identity: *siloed*, *centralised*, *federated*, and *user-centric*.
- Each of the four models describe power relations and interoperability between users, identity providers, and service providers.
- Digital identity systems shape-shift depending on the perspective of the observer and the motivation of their analysis.
- Digital identity cannot be definitively described, because their politics and configurations of power are multi-dimensional.

While the four models of digital identity offer useful terminology to codify digital identity topologies, they are also frustratingly contradictory. Each model contains limitations that affect how we observe and evaluate digital identity. No matter how carefully a digital identity is designed, in practice digital identity resists classification into these neat categories. This chapter examines the blurry boundaries between models that intend to define a given identity system, but remain contingent on *and* influenced by use, legal circumstances, perspective, and technological developments. We apply our working definition of digital identity and interrogate these models alongside Problem Statements I & II that define this research.

This approach allows us to shed new light on contradictions, attack surfaces, complexity, opportunity, and other dynamics shared across each of the four models to set a foundation for our future case studies and intervention work.

~

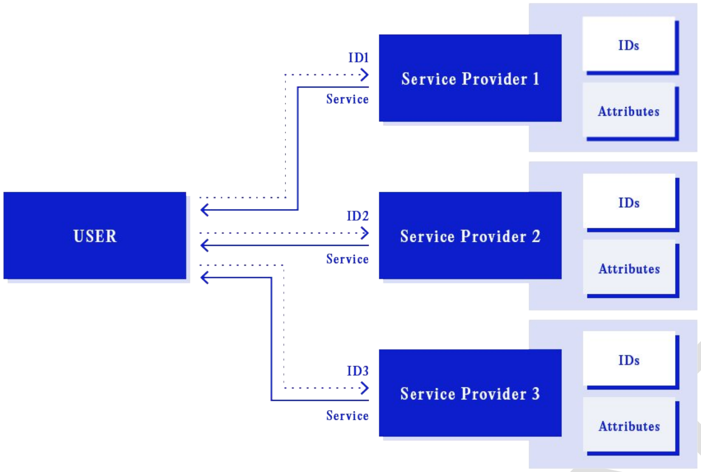
Scholarship on digital identity management systems help us delineate the distinct properties of the aforementioned topologies. In *Digital Identity Management,*[113] authors Laurent-Maknavicius & Bouzefrane introduce the concepts of users, identity providers (IdP), and service providers (SP) to unify the terminology around distinct Digital Identity Management systems:

> *"– a user: a natural person with at least one digital identity wishes to conduct a transaction;*
>
> *– an identity provider (IdP): an entity in charge of digital identity management and of the execution of the authentication mechanism. It enrolls any new user by registering their identifier(s) and some of their attributes. During enrollment, according to its policy, it may be necessary to verify the veracity of the identity provided with the help of an identity card, proof of residence, or even mere proof of receipt of an email;*
>
> *– a service provider (SP): an entity providing users with a service usually a Web service, and relying on the IdP in order to verify the identity given by the user."*

Using these three actor types, Laurent-Maknavicius & Bouzefrane describe four typical models: the siloed model, the centralised model, the federated model, and the user-centric model.

[113] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

The siloed identity model



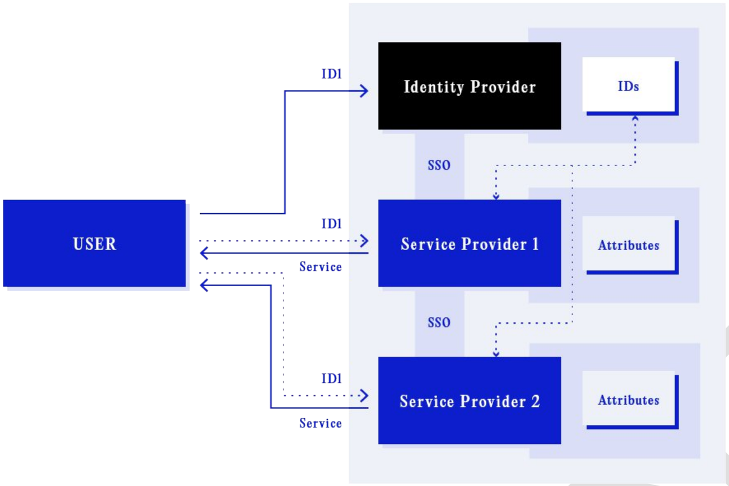
Schematic representation of the siloed model from Laurent et al., p. 34

When a service provides an identity to a user, and this identity is encapsulated to interactions between the two parties only, this is an example of a siloed identity model. The siloed identity is arguably the most familiar to users. A ubiquitous example might be an online store requiring user accounts for customers to make purchases, track orders or contact customer support.

Central to understanding the siloed identity model is its two key characteristics: the service provider is also the identity provider, and the service handles all the authentication and authorisation for the identity. The user creates a new identity for each service they wish to interact with. Each service provider is a different digital identity provider carrying distinct attributes that depend on their specific goals.

User-facing siloed identities usually have well-established user experience flows structured around the creation of a user account, typically via an email address and password. Validation and management of the new account is handled via communication to the user's supplied email address. The tight scope of a siloed identity means a single account is relatively easy for a user to setup and maintain, as their lack of portability or interoperability spares users from the complex privacy or security implications inherent in identity reuse across multiple service providers. For providers, siloed identities are often initially low cost and incredibly easy to implement; their design patterns are amongst the first things learned by systems designers, user experience practitioners, and engineers.

The centralised identity model



Schematic representation of the centralised identity model from Laurent et al., p. 35

When a digital identity provided by one provider is integrated into the system of an unrelated service provider, this is a centralised identity. In this model, the identity provider handles all aspects of design, authorisation, and authentication, and provides methods of integration for external service providers. With a single credential pair, users access different service providers in the system and are represented by the same identity across each platform. This is referred to as Single-Sign On.

Theoretically, the identity provider is always externalised from the the service provider. In all other models, the responsibility for the identity lies partially or wholly with the service provider, or in decentralised cases, the user. In a centralised model, the identity provider is responsible for the design and operation of all authorisation and authentication completed with the identity. This dynamic creates a particular centre of power, where the identity provider becomes a gatekeeper for the access and governance of the identity system over time.

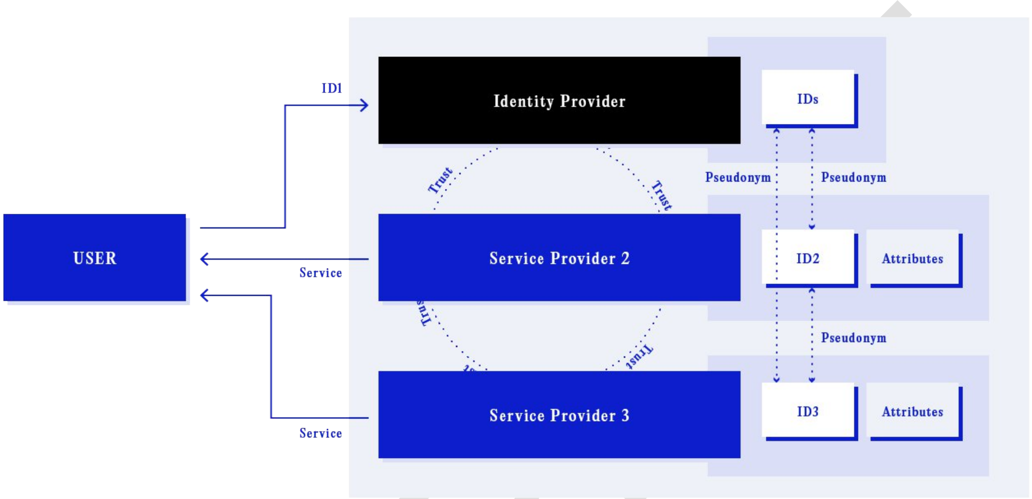
Microsoft Passport[114] is an historical example of a centralised identity. Here, Microsoft leveraged the characteristics of centralised identity in an attempt to position itself as the singular identity provider for the web. The project failed to gain traction due in part to suspicion of Microsoft's motives[115] and the massive power such a system would help, an

[114] Wikipedia, 'Microsoft Account', accessed 16 July 2024, https://en.wikipedia.org/w/index.php?title=Microsoft_account&oldid=1234945749#History.

[115] Declan McCullagh, 'Heading MS Off at the Passport', *Wired*, accessed 22 August 2001, https://www.wired.com/2001/08/heading-ms-off-at-the-passport/.

already powerful company, to accumulate. Microsoft's efforts with Passport led to further theorisation of digital identity systems by Kim Cameron, who in *"Laws of Identity"*, suggested that an identity system would have to accommodate a pluralism of operators and technologies to gain traction.[116] This, in turn, led to the development of the federated digital identity model.

The federated identity model



Schematic representation of the federated identity model from Laurent et al., p. 36

In a federated model of digital identity, the identity provider is separated from the service provider, and the identity is intended to be an interoperable component or protocol within a wider ecosystem.. Because of this interoperability requirement, the federated identity model allows for data exchange across administrative boundaries. Systems that have implemented federated identities allow services outside of an organization's control to authenticate against the organisation's identity provider, given that they meet specific criteria. These conditionals are known as the *circle of trust,*[117]and are an additional key component of federated identity. They require all parties to rely on asserted claims about a digital identity as conveyed by the identity provider within the context of the protocol. The circle of trust can be defined and enforced by legislation, cryptography, consensus, or technological platform, and the negotiated outcome allows individual identity providers to provide

[116] Kim Cameron, 'The Laws of Identity', *Microsoft Corporation*, May 2005, https://www.identityblog.com/?p=352.

[117] 'Liberty Alliance Outlines Legal Framework for Circles of Trust to Comply with European Union Data Protection and Privacy Laws', *Liberty Alliance*, 4 May 2005, https://web.archive.org/web/20100613201457/http://www.projectliberty.org/liberty/news_events/press_releases/liberty_alliance_outlines_legal_framework_for_circles_of_trust_to_comply_with_european_union_data_protection_and_privacy_laws/.

standardised credentials that can be validated by other identity providers or service providers. The federated identity model attempts to balance a higher degree of *control* and *usability* inherent to centralised identity providers against a *decentralisation* of absolute authority over the final design of the identity[118].

Service providers rely on shared consensus to trust the authentication assertions of the identity provider, and the identity provider trusts the service provider to handle the provided user information with care. Kylau et al. describe that *"trust relationships are usually established by a set of contracts defining obligations and rights each party has and policies each member has to follow"* and that setting up such contracts involve *"huge effort"*[119].

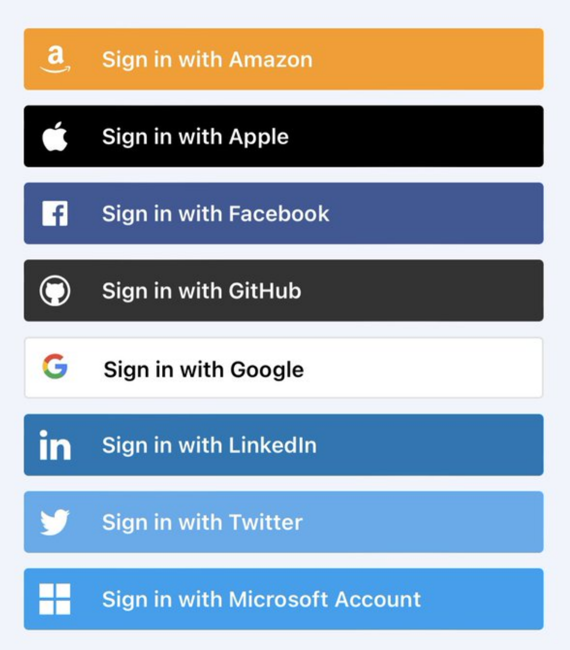
However, using specific protocols for federated identity management makes this substantially easier because the contours of trust relationships are established and defined by these protocols. Since the early 2000s, several successful and widely used examples of federated identity exist, including Security Assertion Markup Language (SAML), and OpenID 1.0 and Open Authentication (OAuth) for authentication.

Federated Identity Management systems built upon these protocols provide standardised and "*unified set[s] of policies and procedures allowing identity management information to be transportable from one security domain to another.*"[120] Users can login to an online store using the federated identity of a large and well-recognised platform–"Login with [Google|Facebook|Microsoft]"– rather than completing the steps necessary to create a new identity and this user experience implies a shared single identity. While this may be true in some implementations, the online store is just as likely to implement its own siloed identity under the hood for the user (described as the Pseudonym in the figure above) and authenticate that against the federated identity provider.

[118] David W. Chadwick, 'Federated Identity Management', in *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*, by Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, Lecture Notes in Computer Science (Berlin: Springer, 2009), 96–120, https://doi.org/10.1007/978-3-642-03829-7.

[119] Uwe Kylau et al., 'Trust Requirements in Identity Federation Topologies', in *2009 International Conference on Advanced Information Networking and Applications*, 2009, 137–45, https://ieeexplore.ieee.org/abstract/document/5076191.

[120] Nitin Naik and Paul Jenkins, 'Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect', in *2017 11th International Conference on Research Challenges in Information Science* (RCIS), 2017, 163–74, https://ieeexplore.ieee.org/document/7956534.



An example of a login screen featuring multiple logos from competing identity providers.[121]

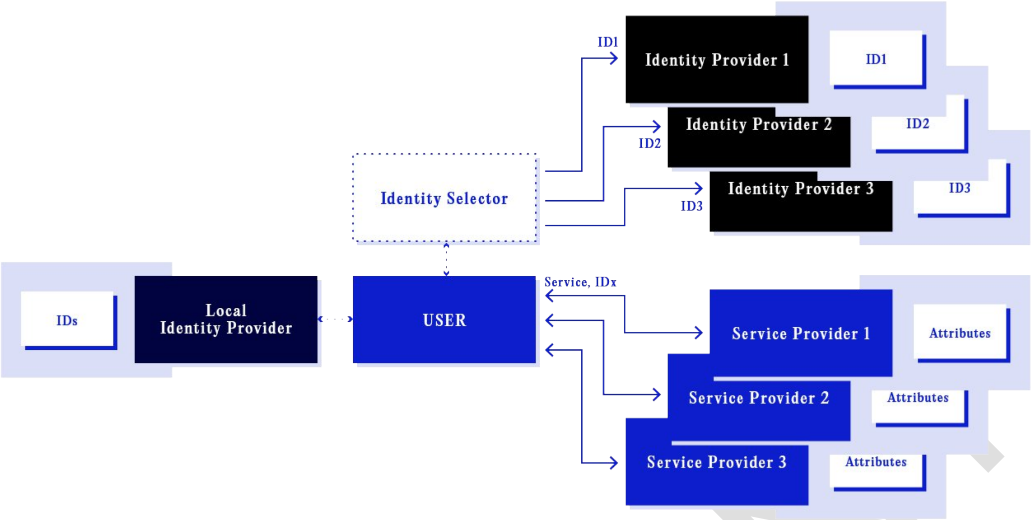
Federated identities have no central authority and anyone can set up an identity provider or implement federated identities into a service provider.[122] Federated identities exist both as a commercial services (Okta, Yubikey, Microsoft Azure) and self-hostable white-label technologies that can be implemented in a new or existing application (Keycloak, Authentik). Finally, federated identity models allow Service Providers to configure multiple identity providers, broadening the likelihood that a user has a pre-existing account with one of several authentication options offered. Depending on the which federated identity the user elects to use, this can have wildly unpredictable data privacy implications, as users are forced to trust service providers to respect their privacy as they receive and process an offered identity credential.[123]

[121] Stevə [@Northvein], 'When Did This Become Normal?', *X*, 6 October 2021, https://x.com/Northvein/status/1445640353084633088.

[122] Pauli Kaila, 'Oauth and Openid 2.0', in *Proceedings of the Seminar on Network Security*, vol. 18, (From End-To-End to Trust-to-Trust, Espoo: Helsinki University Of Technology, 2008), 18–22, http://www.cse.tkk.fi/en/publications/B/4/netsec08-proceedings.pdf.

[123] Maryline Laurent et al., 'Digital Identity', in *Digital Identity Management*, ed. Maryline Laurent-Maknavicius and Samia Bouzefrane (London: ISTE Press, 2015).

The user-centric identity model



Schematic representation of the user-centric identity model from Laurent et al., p. 37

When a digital identity is derived entirely from the user, or the user also acts as the identity provider, this is considered a user-centric digital identity model. This approach often—but not always—emphasises user autonomy and contrasts with traditional identity management systems, where control is typically centralised with service providers or institutions. For Laurent-Maknavicius et al., the key aspects of a user-centric identity include user-led control, attribute compartmentalisation (framed as privacy protection), interoperability, and full decentralisation[124].

In one common example of user-centric identity, a user actively develops and manages their identity attributes through a local identity provider, selectively disclosing information to various service providers based on their preferences and the specific context of each interaction. In practice, several protocols, such as OpenID 2.0 and OpenID Connect, have been developed to facilitate this process. These protocols combine authentication and authorisation, allowing users to authenticate across administrative boundaries while disclosing only a limited amount of identity attributes, such as a profile picture and email address.

Performative identity is another example of user-centric digital identity, where an identity is enacted or performed through user actions and interactions. In this case, users deploy

[124] Maryline Laurent et al., 'Digital Identity', in *Digital Identity Management*, ed. Maryline Laurent-Maknavicius and Samia Bouzefrane (London: ISTE Press, 2015).

context-specific personas and engage in active compartmentalisation of their identity when interacting with other users or service providers.

Finally, user-centric identity can also be derived from user characteristics, where individual user behaviour, physical characteristics, or digital footprints become aspects in assembling a unique and recognisable identity. Here, the implied user empowerment inherent to user-centric digital identity is inverted despite the model adhering to the conditions of the model at a surface level.

~

From Models to Spheres

In the previous two Problem Statements, we examine systemic flaws in the conceptualisation and administration of digital identity and their broader societal consequences. The practice of modelling and evaluating digital identity contain similar shortcomings that contribute to the weakening of digital identity. At its core is a key flaw: the evaluation model(s) for a digital identity shifts over time, based on the observer's motivations, perspective, and beliefs. The amorphous nature of applied digital identity models conflicts with the rigid requirements of evaluation. Multiple contradictory frameworks can be employed simultaneously to a single digital identity system, creating blurred boundaries and tensions between theoretical frameworks and practical implementations.[125]

Since identity models can overlap and coexist, we need a new language and approach to digital identity management. This is a situation that is aggravated as best-practices and historical decisions are layered on top of each other. **To address these issues, we propose the concept of *spheres of identity*, which accommodates a more flexible and adaptive approach to identity evaluation, moving beyond the rigidity of today's best practice.**

~

The trade-offs of the siloed identity model best exemplify the issues that arise from the shortcomings of digital identity modelling. As the oldest and most widespread model, siloed identity is defined by the fact that all facets of control, custodianship, governance and responsibility[126] is solely held by the dual identity/service capabilities of the provider. This

[125] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee, 'The Identity Crisis Security, Privacy and Usability Issues in Identity Management', arXiv, 2 January 2011, https://arxiv.org/abs/1101.0427

[126] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

model is particularly suitable for representing non-human entities or implementing application-specific attributes and identifiers, allowing systems designers to model and plan interactions with computers and processes according to specific protocols or behaviours. However, managing multiple isolated identities can become an unreasonable challenge, especially for infrequent services such as annual tax reporting or occasional online shopping.[127]

Users are often asked to use their email address as their unique identifier, creating a subtle but important cognitive link between discrete, non-interoperable siloed identities. To manage the complexity of an ever-increasing repository of siloed identities, users frequently resort to password reuse, which decreases the complexity of identity management for themselves. The reuse of credentials can thus be understood as a form of DIY portability deployed to mitigate the core limitations of the non-portable properties of the siloed identity model. Ethnographic work on sociotechnical systems has extensively documented the way people use and need work-arounds,[128] kludges,[129] and other patches to be able to make effective use of systems, and this DIY portability is an example of this.

User-driven DIY-portability has major consequences. When compromised, DIY-portable credentials also become DIY-portable tools for attackers. Credential reuse in siloed identities is now a major attack surface for cybercrime. A large-scale data breach of one provider's identity system unlocks cascading access to other providers, and the user must respond individually to each instance of credential reuse. Where siloed identities lack interoperability and do not share global namespaces between identity/service providers, the 'user-led' soft-patch of credential reuse creates an ad-hoc global namespace that allows attackers to traverse multiple isolated platforms, testing credentials and compromising these unrelated identities.[130] Thus, a theoretically siloed model in practice becomes centralised and portable over time.

An ad-hoc alternative to credential reuse is the use of password managers, where a user self-manages a single master identity that grants access to a secure personal database containing all other credentials. When practised with a high degree of discipline, this

[127] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov and XiaoFeng Wang, "The Tangled Web of Password Reuse," in *Proceedings of the 2014 Network and Distributed System Security Symposium* (San Diego, 23-26 February 2014), 3-6, https://www.ndss-symposium.org/wp-content/uploads/2017/09/06_1_1.pdf.

[128] Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power*, 4. print., paper (New York, NY: Basic Books, 1992).

[129] Philip Koopman and Robert R. Hoffman, 'Work-Arounds, Make-Work, and Kludges', *IEEE Intelligent Systems* 18, no. 6 (2003): 70-75, https://ieeexplore.ieee.org/abstract/document/1249172/?casa_token=duvGsGwuMtwAAAAA:3ttk63Kl_8Q6inpJamAtQ7iVOiNQdlDhFsnL6zqcJ7BsULyB_yCbKe8I_kr-YPvPdODE6V8odr5g.

[130] Kurt Thomas et al., 'Protecting Accounts from Credential Stuffing with Password Breach Alerting', *Usenix Security,* 2019, 1556-71, https://www.usenix.org/conference/usenixsecurity19/presentation/thomas.

method allows for the use of unique usernames and randomly generated passwords that user does not have to remember. In the case of a data breach, the cascading access to other providers through credential reuse or DIY portability does not occur.[131] At the same time, the user must only commit a limited number of credentials to memory. In such a scenario, theoretically siloed identities remain siloed in practice, but 'soft-managed' by an external centralised identity – the password manager.

Despite the security risks associated with ad-hoc portability, the siloed identity model offers significant advantages for user agency, 'consent'[132] and privacy. Its encapsulated nature allows users to deliberately create *performative identities* in order to share only aspects of their identity or assume others, or maintain a form of defensive control over, and compartmentalisation of, the identity by creating *identity personas* to minimise spam and defend against profiling.

For instance, users might create temporary e-mail addresses or disposable identities for activities such as exploring sexual, gender, and other marginalised aspects of identity or engaging in political debate, as well as avoiding unsolicited marketing material. The siloed identity model allows users to compartmentalise identity attributes to different services, exposing only the minimally required amount to get access to a particular service. This is especially the case in combination with the use of password managers and temporary e-mail addresses. By compartmentalising identity attributes, users can expose only the minimally required information to access specific services, aligning the siloed model with user-centred identity principles.

Performative user-centric identities can be user-driven statements of self- curation and representation in a digital system. Erving Goffman's *identity performance* concept, draws on the assumption or understanding that identity is not a fixed attribute but a performance that can vary across different contexts. In digital environments, users actively construct and manage their identities to suit specific interactions, audiences, and purposes.[133] Pseudonyms, digital avatars, and digitally-derived real world pseudo-identities (such as fursonas[134]) are all examples of performative identity.

[131] Carlos Luevanos et al., 'Analysis on the Security and Use of Password Managers', in *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies [PDCAT]*, 2017, 17–24, https://ieeexplore.ieee.org/document/8326801.

[132] Cade Diehm et al., 'The Limits to Digital Consent: Understanding the Risks of Ethical Consent and Data Collection for Underrepresented Communities', *Simply Secure and New Design Congress*, 25 October 2021, 21, https://simplysecure.org/resources/The_Limits_to_Digital_Consent_FINAL_Oct2021.pdf.

[133] danah boyd, 'Faceted Id/Entity: Managing Representation in a Digital World', *Massachusetts Institute of Technology*, 2002], https://dspace.mit.edu/handle/1721.1/39401.

[134] Jakob W Maase, *Keeping the Magic: Fursona Identity and Performance in the Furry Fandom,* [Western Kentucky University, 2015].

In some ways, identity personas share conceptual motivations with performative identity. But whereas the performative is driven by play or a desire to project oneself into the digital world, personas emerge when users strategically compartmentalise their identity as a form of defensive security.[135] Identity personas allow individuals to create multiple, distinct curated identities for various online interactions, thereby limiting the exposure of personal information and reducing the risk of identity-related threats. Each persona can be tailored to specific contexts, such as professional networking, social media, or online shopping, ensuring that only relevant information is shared with each service provider. In this way, users exert a level of control over data leakage across multitudes of service providers. These strategies can be employed across a number of identity models, but can fall apart when used on top of a centralised identity.[136]

~

The use of multi-factor authentication (MFA) has emerged as an additional layer of defence to address some of the faults of the siloed identity model. There are a variety of MFA implementations, including physical hardware keys, application-based TOTP (e.g., Authy, FreeOTP, and Google Authenticator), SMS codes sent to a user-nominated phone number, user-supplied biometric scans, or linking the siloed identity to an out-of-band centralised identity. Regardless of the method, the goal of MFA is to validate user ownership of an identity by proving access to another, introducing enough friction to disincentivise an attacker while remaining user-friendly.

MFA is a challenge that further complicates the siloed digital identity, as different implementations establish various dependencies and soft-links between identities. For example, an SMS-based MFA is tied to a phone number is an example of a centralised identity. Similarly, a hardware MFA key may be derived from a federated protocol. Soft-links create intentional barriers of access for the siloed identity, and once introduced, cannot be conceptually separated. The identity model of the soft-linked MFA influences the relationships between the user, identity providers, and service providers.

Service providers often struggle to distinguish genuine human siloed identities from automated equivalents that are often adversarial.[137] As a result, many services incorporate

[135] Yannis Juglaret et al., ‘Beyond Full Abstraction: Formalizing the Security Guarantees of Low-Level Compartmentalization’, ArXiv, 14 February 2016, https://www.semanticscholar.org/paper/Beyond-Full-Abstraction%3A-Formalizing-the-Security-Juglaret-Hri%C5%A3cu/3ca938c990c684ec4e29d2d132bf2e5ef9c2f771.

[136] An illustrative example of this falling apart is when the *People You May Know* feature launched on Facebook, many performative identities and personas became visibly linked to one another as the system started recommending personas to people who otherwise intended to keep them secret and separate. https://gizmodo.com/people-you-may-know-a-controversial-facebook-features-1827981959

[137] Stephanie Edgerly and Emily Vraga, ‘The Blue Check of Credibility: Does Account Verification Matter When

steps that provide rudimentary ad-hoc proof-of-personhood. These measures, such as highly inaccessible CAPTCHAs[138] or device sensor surveillance,[139] aim to verify human presence but can also lead to the creation of shadow identities sold to data brokers.[140] In these cases, are the automatically generated profile or the credentials used to access a service the actual identity in use? The answer is often unclear.

Beyond proof-of-personhood, service providers that rely on siloed identities often work from a *one user, one account* design that assumes the digital identity represents a single individual.[141] In practice, service providers are almost always unable to determine whether one user has multiple accounts or whether multiple users are using one account. While tying a specific person/user to each account may be required for some services and specific industries, such as banking and telecommunications that must adhere to Know Your Customer (KYC) regulations, this does not ensure the accuracy of attestation of identity.

Shared siloed identities can also have serious implications: the actions of one individual using a shared account may have platform-based or real world consequences for another individual who is legally bound to the digital identity. A 2024 exposé on automated identification and targeting systems used by the IDF underscores how the *one user, one account* model has disastrous outcomes for those wrongly identified. Speaking to +972 Magazine, a source familiar with these operations describes the consequences: *"In war, Palestinians change phones all the time. [...] People lose contact with their families, give their phone to a friend or a wife, maybe lose it. There is no way to rely 100 percent on the automatic mechanism that determines which [phone] number belongs to whom."*[142]

~

The blurred boundaries and simultaneous applicability of different identity models extend beyond the siloed model to centralised and federated models. The key differentiator of the

Evaluating News on Twitter?', *Cyberpsychology, Behavior, and Social Networking* 22 (8 March 2019), https://www.liebertpub.com/doi/10.1089/cyber.2018.0475.

[138] Meriem Guerar et al., 'Gotta CAPTCHA 'Em All: A Survey of 20 Years of the Human-or-Computer Dilemma', *ACM Computing Surveys* 54, no. 9 (8 October 2021): 192:1-192:33, https://dl.acm.org/doi/10.1145/3477142.

[139] Weijun Qin et al., 'Discovering Human Presence Activities with Smartphones Using Nonintrusive Wi-Fi Sniffer Sensors: The Big Data Prospective', International Journal of Distributed Sensor Networks 2013 (1 December 2013), https://journals.sagepub.com/doi/10.1155/2013/927940.

[140] David Garcia, 'Leaking Privacy and Shadow Profiles in Online Social Networks', *Science Advances* 3, no. 8 (4 August 2017), https://www.science.org/doi/10.1126/sciadv.1701172.

[141] Max Edwards, "ISO 27701 – Clause 6.6.2 – User Access Management," *ISMS.online*, 25 February 2025, https://www.isms.online/iso-27701/clause-6-6-2-user-access-management/.

[142] Amjad Iraqi, '"Lavender": The AI Machine Directing Israel's Bombing Spree in Gaza', *+972 Magazine*, 3 April 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

centralised model was the separation of identity provider from service provider. In the federated model the identity provider can be used across administrative domains.

Historically, the centralised and federated models have been distinct, but modern identity management software has blurred these differences over time. Federated identity systems are implemented in universities or other large organisations as a single credential, providing a variety of in-house or external resources to users. The ability to link multiple services together via a single user authentication flow is known as Single Sign-On (SSO), where a user supplies a single set of credentials (e.g., username and password, sometimes with MFA) to authenticate against different services. Federated identity systems such as, OpenID, OAuth, OpenID Connect, establish a *Circle of Trust* through technical means rather than organisational agreements to allow for Single Sign-On. At the same time, they can make a federated digital identity indistinguishable from a centralised identity. To complicate matters more, later versions of OpenID and OpenID Connect have been designed to be *user-centric* systems, but are often implemented in centralised or federated fashions.

A key property of the federated model is that credentials remain with the identity provider, with only necessary attributes shared with the service provider. This theoretically enhances privacy compared to the required hosting required for centralised or siloed identities. Users benefit from using a limited number of identity providers to access a larger amount of service providers. However, in practice, the difference between identity provider and service provider is not as strict as the theoretical models present it. The examples of Login with Google and Login with Facebook demonstrate how identity providers can simultaneously be service providers who specifically base their mode of operation on user data surveillance. This can have consequences for user privacy, as these identity providers can gain insights on a user behaviour they would otherwise not have access to, if the user did not use the identity provider as a login mechanism. This dynamic is not fully captured in theoretical models.

Furthermore, the relationship between dual identity/service providers and federated identity providers tends to be uni-directional. While users can use Google as an identity provider for a local online store, the reverse is not typically possible. This asymmetry highlights the need for a more nuanced understanding of identity models, recognising the evolving interplay between centralised, federated, and siloed systems.

Because the dynamics of service and identity providers remain unaddressed, digital identity systems in the consumer internet space have consolidated into a handful of providers such as Google or Facebook.[143] The concentration of power is further aggravated by the so-called *NASCAR problem*, named after the many corporate logos that adorn sponsored racing cars. Here, a service provider's login or sign up interface features a gallery of logos, each representing different compatible identity providers to authenticate with. Like the shortcuts of credential reuse in siloed identity, users take shortcuts to reduce complexity. The amount of choice leads people to opt into familiar or recognisable brands.[144] As a result, large commercial technology providers have seized on user behaviour to become global centralised digital identity providers.

As federated models centralise, centralised models federate. The widespread deployment of state-backed national e-ID schemes in Northern Europe provide good examples of centralised identities that become interoperable across organisational boundaries. In Sweden, BankID operates as a *platform-of-platforms*,[145] offering both proof-of-personhood and centralised digital identity management via API endpoints and legislation. Administered by a single corporate entity owned by Sweden's largest banks, BankID's proof-of-personhood is backed by each bank's KYC procedures, which in turn relies on government identity systems. BankID is used to authenticate against a wide variety of both public and private service providers, ranging from payment providers to insurers to the tax office and the social welfare system.[146]

Understanding these dynamics in terms of spheres rather than as rigid models is unconventional, but allows for seemingly counter-intuitive (yet justified) claims when evaluating digital identity. Hence, the following examples of topologically diverse systems can still be considered to belong to the centralised sphere:

- Identities embedded in hardware tokens or access cards, such as Yubikey's MFA keys or HID Global's suite of products, including employee identification cards that provide building access, and government-issued biometric passports;

- Tunnelled identities, where the identity is embedded in open source connection security protocols, such as OpenVPN or Wireguard. Examples include Tailscale,

[143] Harry Halpin, 'Decentralizing the Social Web: Can Blockchains Solve Ten Years of Standardization Failure of the Social Web?', in *Internet Science*, ed. Svetlana S. Bodrunova et al., vol. 11551 [Cham: Springer International Publishing, 2019], 187-202, https://link.springer.com/chapter/10.1007/978-3-030-17705-8_16.

[144] 'NASCAR Problem', Indieweb Wiki, 3 June 2022, https://indieweb.org/wiki/index.php?title=NASCAR_problem&oldid=81810.

[145] Claire Ingram Bogusz and Harris Kyriakou, 'Digital Identity as a Platform of Platforms : Investigating Bankid's Effect on Swedish Organizations', *ECIS 2023: European Conference on Information Systems, Kristiansand, Norway 2023*, Association for Information Systems, June 11-16, 2023, https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-500335.

[146] Ben Eaton et al., 'Achieving Payoffs from an Industry Cloud Ecosystem at BankID', *MIS Quarterly Executive* 13, no. 4 [28 November 2014], https://aisel.aisnet.org/misqe/vol13/iss4/6.

where the centralised identity is cocooned within a secure virtual network connection and integrated into a service provider;

- Blockchain/Web3 identities, where the user identity is tied to a token or other value store, and the identity is considered portable via a common underlying protocol (such as Ethereum), or via conducting transactions between two parties to move the identity between implementations;[147]

- Identities based on messaging protocols, where the identity is returned after an automated system makes contact with a user via a messaging platform with a one-time code and the user completes a sign in or sign up process using that code. These are rapidly expanding, such as Telegram's third party authentication system or services that advertise *passwordless* sign up by providing authentication links via email; or

- Identities derived from existing standardised SSO implementations, usually OAuth, LDAP or OpenID Connect. Such identities are distinct in that they operate *only* as an identity provider. For example, the Berlin BVG public transportation company manages its passenger accounts and ticketing with the assistance of an identity primitive derived from the Keycloak open source project,[148] and has a degree of interoperability with other public transport, taxi services and ride share providers within Germany. Other examples include Okta's Identity Cloud and the open source Authentik project.

~

Research on digital identity management systems has identified several models – siloed, centralised, federated, and user-centric – each with distinct properties and a historically progressive trajectory. **Each model builds on, and improves, the shortcomings of its predecessors. However, in practice, the clear delineations of these ideal-typical forms blur, contributing to the discrepancies when trying to reckon with the failings of digital identity systems.**

To address these discrepancies, we propose shifting from rigid identity management models to "spheres" of identity, advocating an approach that accommodates the amorphous nature of digital identity and, crucially, embraces

[147] Consider, for instance, Moxie Marlinspike's reflections on the platformisation of blockchain systems: https://moxie.org/2022/01/07/web3-first-impressions.html

[148] Although little has been made public about BVG's use of Keycloak, the source of BVG-Konto is identifiable as being based on the project. An example can be found here: https://www.bvg.de/de/bvg-konto

the multitudes inherent in each identity system. This means observing and describing topologies as they truly are, rather than as they are purported to be, and developing methods that allow for discrepancy or contradiction at a fundamental level. As we witness a widespread push for novel identity systems that aim to address the perceived shortcomings of earlier generations, this reconsideration becomes particularly pertinent. **It is essential to question whether older generations of identity systems allowed for more flexibility and whether newer systems have genuinely overcome the limitations of their predecessors.**

We challenge the topological determinism often found in both technical builders and critics of digital systems. Conceptualising a particular identity system as fitting a specific topological model obscures attack vectors and vulnerabilities typically associated with other models. **To adopt a more fluid approach to identity evaluation is to make sense of the complex and messy terrain of digital identity systems. We must embrace the spheres of identity as an inescapable requirement for rethinking the first principles of digital identity if we are to implement resilient representations in uncertain and unstable societies.** ✳

Research Methodology

This research project commenced in November 2022 as an internal inquiry into the socio-technical vulnerabilities inherent in modern digital identity systems. Over the course of the project's timeline, the research grew in scope due to the systemic nature of digital identity, through the inclusion of external stakeholders, and the research opportunities contributed by experts who participated in the qualitative interview component of the research.

This report is informed by prior work by New Design Congress, including:

- *Backchannel,*[149] in which the researchers designed and prototyped a relationship-based digital identity framework in collaboration with the Ink & Switch research lab;
- *The Limits to Digital Consent,*[150] a report co-published with Simply Secure that found ongoing attempts to cultivate informed consent into data-driven systems often fall short of their stated goals;
- *Memory in Uncertainty: Web preservation in the polycrisis,*[151] which found numerous examples of multi-faceted threats posed by digital identity in the context of data custodianship and digital archiving;
- *This is Fine: Optimism and Emergency in the P2P Network,*[152] a New Design Congress text that summaries the un-addressed threats faced by decentralised and federated networks;
- *The Imperial Sensorium,*[153] a New Design Congress foundational text that critiques Cybernetics as a severely limited model of sensing and understanding the material world;

[149] Karissa Rae McKelvey et al., 'Backchannel: A Relationship-Based Digital Identity System', *Ink & Switch*, 1 September 2021, https://www.inkandswitch.com/backchannel/.

[150] Cade Diehm et al., 'The Limits to Digital Consent: Understanding the Risks of Ethical Consent and Data Collection for Underrepresented Communities', *Simply Secure & New Design Congress*, 25 October 2021, https://simplysecure.org/resources/The_Limits_to_Digital_Consent_FINAL_Oct2021.pdf.

[151] Cade Diehm and Benjamin Royer, 'Memory in Uncertainty: Web Preservation in the Polycrisis' *New Design Congress, November 2022*, https://newdesigncongress.org/en/report/2022/memory-in-uncertainty/.

[152] Cade Diehm, 'This Is Fine: Optimism & Emergency in the P2P Network', *New Design Congress,* 16 July 2020, https://newdesigncongress.org/en/pub/this-is-fine.

[153] Benjamin Royer, 'The Imperial Sensorium', *New Design Congress*, 21 June 2022, https://newdesigncongress.org/en/pub/the-imperial-sensorium.

- *The Para-Real: A manifesto,*[154] a supporting New Design Congress research project that examines the transformative power inherent when digital identity is paired with the material or socio-technical lived conditions of an individual user, and;

- *Decentralised social media,*[155] a journal article for the Internet Policy Review's *Glossary of decentralised technosocial systems* that defines different models for centralised, federated and decentralised social media platforms.

Following an extensive landscape review the researchers defined a working definition of digital identity and four problem statements that represent consistent systemic flaws in varying design and implementation of digital identity.

Between February 2023 and August 2024, the researchers identified and approached a range of experts whose work either focused on or intersected with digital identity systems. When assessing who to approach, potential candidates needed to fulfil one or more key criteria. Candidates needed to:

- Have designed, implemented, or evaluated a digital identity system from a technical, political or information security background;

- Had campaigned for or against a digital identity system as an activist, for example concerning the privacy or weaponisation of digital identity or the promotion of self-sovereign identity;

- Been responsible for, or had participated in, legislative process related to digital identity;

- Held a role as a third party observer in contexts where digital identity played a major role, such as election integrity or digital forensic practices;

- Interacted with digital identity implementations within legal contexts, or;

- Been targeted by a novel cybersecurity attack that utilised digital identity as a core component of the event.

[154] Cade Diehm, 'The Para-Real: A Manifesto', *New Design Congress*, 10 December 2022, https://newdesigncongress.org/en/pub/the-para-real-manifesto/.

[155] Roel Roscam Abbing, Cade Diehm, and Shahed Warreth, 'Decentralised Social Media', *Internet Policy Review* 12, no. 1, 20 February 2023, https://policyreview.info/glossary/decentralised-social-media.

Significant efforts were made to ensure diversity of gender and sexual identity, race, cultural, and socio-economic status. Efforts were also made to ensure institutional archiving participants were not overrepresented in the study.

Specific conditions created challenges to ensuring the realities of differing digital identity systems were represented and to reduce bias in the research. These included:

- Deliberate actions by the researchers to recruit participants from a wide variety of backgrounds;
- Screening potential participants through a short and accessible application form;
- Where appropriate, sharing early findings and generalised demographics with members of the New Design Congress community for feedback, and;
- The deliberate use of accessibility and privacy tools alongside clear language data custodianship policies to increase the likelihood of participation by at-risk and marginalised participants

The majority of research participants were industry professionals, cryptographers, activists, journalists, law enforcement, artists, members of the military and intelligence communities and policy-makers or international independent observers, with a minority being end-users rather than holding positions within the digital identity landscape. Almost all research participants spoke English, with a very small subsection interviewed with translation assistance. Male-identifying participants were overrepresented amongst the digital security and law enforcement demographic.

This categorisation remains a simplification for expediency and the security of participants, and does not hope to provide any precise metrics beyond inferring certain biases in the research. It also doesn't reflect the individual heritage of each participant and its associated influences. The surfacing of such complex interplay of identities, origins and intersectional interests remains the role of the interviews and the subsequent report.

These interviews continued throughout the duration of the research timeline. Interviews were conducted either in person or via platforms selected individually by each research participant and facilitated by two researchers – one acting as the interviewer, and the other supporting and note-taking. Additional interviews took place in February 2023 in Taiwan, Japan and South Korea as part of an early exploratory phase of the research project.

The interviews were recorded locally by both researchers using OBS Studio, avoiding cloud-based recording features available in services such as Zoom, Signal and Jitsi. Although interviews were conducted via video, only audio was recorded. Participants were asked to consent to the interview in advance via the Research Consent Form (see Appendix C).

Sensitive to the constraints of participants, the research interviews were between 60–120 minutes in length and structured via a series of key questions that reflected the broader research focus (see Appendix B). Participant responses guided the direction of each interview, and the key questions were not always followed sequentially. Recordings of each interview were transcribed and anonymised, before being synthesised as part of the research findings. As per the Research Consent Form (Appendix C), each participant has been offered the chance to review their contribution and withdraw or affirm their participation consent before publication. The original audio files were destroyed at the conclusion of the research project.

Before publication, two participants withdrew from the study.

Finally, the research project adheres to New Design Congress' Privacy Policy, Methodology and Code of Conduct, all of which are available online at https://newdesigncongress.org/en/methodology. Funding declarations can be found at the end of this report. ✳

Key Findings

1. Ambiguity in defining digital identity hinders cohesive industry and policy action

In 2019, ISO ratified ISO/IEC 24760-1:2019 with an authoritative definition of digital identity. This is the standard most often cited by institutions. While technically accurate – *an identity can, in fact, be a set of attributes related to an entity*[156] – the phrase is both definitive and remarkably empty: it says as little as possible, as broadly as possible, and appears to be designed for as many stakeholders as possible. It is also *incomplete*; As a product of Western rationalist tradition, the ISO definition both denies other forms of identity possible within digital systems, and ignores how digital identity shifts when it is perceived or interpreted by a system. A cynical reading might suggest this emptiness is deliberate: by saying almost nothing, the standard grants vendors and governments carte blanche to claim compliance while ignoring substance.

Key Points

- › Digital identity lacks a universal definition, with interpretations shaped by political, technical, and cultural agendas.|
- › Competing frameworks make consensus impossible. Identity is seen as protocol, performance, and proof all at once.
- › Market hype cycles from smartphones to LLMs continually reshape what identity means and how it's used.
- › Trust is foundational but fractured, varying wildly between technical, institutional, and human contexts.
- › This ambiguity fuels social engineering and turns identity systems into coercive infrastructure.

The ISO working group included representatives from Microsoft, Oracle, IBM, and major defence contractors,[157] [158] [159] entities whose business models depend on definitional flexibility. By crafting a standard that says nothing while appearing authoritative, the resulting ambiguity-as-technical-guidance creates a grey area in which any and all forms of digital identity can be projected. In practice, this is, perversely, what makes the ISO definition so useful: it is the empty centre around which everyone in the field improvises.

[156] International Organization for Standardization, *ISO/IEC 24760-1:2019 IT Security and Privacy – A Framework for Identity Management – Part 1: Terminology and Concepts*, 2nd ed. [Geneva: ISO, 2019], https://www.iso.org/standard/77582.html.

[157] American National Standards Institute, *ANSI Board of Directors 2023 Roster* [PDF], 2023, https://share.ansi.org/Shared%20Documents/About%20ANSI/Governance/ANSI-ExCo-Roster.pdf.

[158] British Standards Institution, "Microsoft Sets a High Bar for Information Security", 2015, https://www.bsigroup.com/LocalFiles/en-US/Case-Studies/Microsoft_CaseStudy.pdf.

[159] DIN – Deutsches Institut für Normung, "DIN Membership Network," accessed 30 July 2025, https://www.din.de/en/getting-involved/din-membership.

Over four years of research into digital identity, and having reviewed hundreds of definitions, **we found that authors, researchers, policy-makers, and systems designers regularly include a definition of digital identity that satisfies their immediate motivations, interests, objectives, or political context.** The irony, of course, is that this is true even of this research project. In order to interrogate the ***first principles of digital identity*** against the ***three problem statements***, we require our own working definition of digital identity. We have yet to uncover a reliable, universal, or authoritative definition for digital identity. Points of contention remain: the inclusive nature of digital identity, the limitations inherent to digital identity, and the classification of digital identity as conceptual or material. This key finding has vast implications for how digital identities affect the wider world.

~

In *The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity* (2023), Kirsty Innes, Jeegar Kakkad, and Ryan Wain of the Tony Blair Institute for Global Change described digital identity as inherently self-sovereign:

> *"There is no way for individuals to control how information is shared between different parts of government. By contrast, well-designed digital infrastructure would give people control of their data, make it easier and quicker to prove their eligibility for needed services and, in turn, allow those services to be personalised to individual needs. This digital infrastructure would need to be developed and delivered in close collaboration with the private sector and civil society."*

Echoing other governmental advisors and think tanks, the authors invoke the ***taxonomy of financialisation*** – in this case, ***wallets*** – as the core vehicle of digital identity transactions between users and service providers: *"The wallet could be used to gain access to personal data held in various parts of government. People could also use it to agree to privately and securely share data to produce collective aggregated data sets that could be used to draw insights about all sorts of government functions and services."*[160]

In contrast, Thales Group, a multinational defence and infrastructure contractor, describe the plurality of digital identity and define the concept strictly within the bounds of existing digital protocols:

[160] Kirsty Innes, Jeegar Kakkad and Ryan Wain, The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity, *Tony Blair Institute for Global Change*, 15 June 2023, https://www.institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.

“The most common form consists of an email address and a password to access different online services. In this case, they are not verified and, therefore, not trusted. It is critical that user identity is verified and trusted when it comes to sensitive services such as government, financial services, mobile communications and a whole host of others.”

From their perspective, the ideal digital identity is immutable and trusted:

“A trusted digital identity provides the ability to prove that the person or device trying to access a service is the one for whom the service is provided, and is vital to the development of online services and seamless experiences when interacting in digital space.”[161]

What counts as a digital identity changes drastically, whether driven by the whims of market forces or technological trends. Since the release of ChatGPT, and other machine learning large language models, digital identity has been redefined as an assistance tool to be leveraged in online interactions on behalf of a user. This trend was observed both in the wider landscape of digital identity and amongst research participants. For example, one participant described a desire for large language models to represent users in healthcare negotiations:

‘For an elderly population on social insurance, expecting them to pick up their smartphone, and negotiate identity sharing and consent when they’re just trying to get a prescription refill, those are all present challenges. And where I’ve been involved in discussions in the U.S. specifically around consent [...], to say how are you consenting to share your data within the confines of how it’s kept right now? Consent solutions can be complicated, and we worry about consent fatigue, where a system comes back and asks me 30 questions [...]. And I think anyone of us would just go default yes after a while because we’re trying to watch a movie and we don’t have time to answer. But at that point, we have to consider: where does autonomous AI and personal AI assistance come in to do some of that heavy maths and give you in plain language: “we think that it’s okay to share X, Y, and Z. We recommend you share it for this period of time.”’

In the wider landscape, examples of large language models acting as identity representatives abound – if greeted with incredulity. In 2024, Zoom CEO Eric Yuan claimed users would represent themselves in white-collar meetings via ***AI clones*** that mimic their identity and can be entrusted to make decisions on the their behalf.[162] While

[161] Philippe Vallée, “What Is Digital Identity, and Why Is It Important?” *Thales Digital Identity & Security Blog*, 18 June 2021, https://dis-blog.thalesgroup.com/identity-biometric-solutions/2021/06/18/what-is-digital-identity-and-why-is-it-important/.

[162] Nilay Patel, “Zoom CEO Eric Yuan Wants AI Clones in Meetings,” *The Verge*, 3 June 2024,

widely ridiculed, the AI tech scene is awash with competing products and platforms making similar claims: ***where the service is positioned as a digital extension of the self***.

Historically, there are a number examples of revisions redefining digital identity in response to market forces. Perhaps the most dramatic is the surging popularity of the iPhone throughout the 2010s, which in turn influenced socio-cultural and academic thinking around the conceptual relationship between digital identity and the self. In many cases, the definition of digital identity, in the 2010s, was constantly shaped by the capabilities of then current-gen smartphones. In *Discourse, cybernetics and the entextualisation of the self,* Rodney H. Jones describes digital identity as the entanglement of hardware and the quantified self:

“Historically, digital identity has been partially entangled with hardware, particularly smartphones. More and more I find myself emotionally attached to my iPhone, not so much as a communication device, and not as a physical object that expresses my identity and social status […], but, rather, as a ‘servomechanism’, a means for receiving constant feedback about my physical and mental well-being.”[163]

Alongside policy think-tanks and technology platforms, academics and researchers have often defined digital identity through the immediate context of market forces, personal motivations and other trends: in *The Stack: On Software and Sovereignty*, a text published at the peak of the 2015-era smart city and internet of things hype-cycles, Benjamin Bratton defined digital identity as part of an esoteric ‘planetary-scale computation.’ Here, Bratton haphazardly assembles digital identity via layers of *‘Earth,’ ‘Cloud,’ ‘City,’ ‘Address,’ ‘Interface,’* and *‘User,’*[164] a set of properties that (coincidentally) correspond neatly with the data dependencies of the smart city and internet of things.

Yet even market-driven definitions contradict each other. In a subsequent chapter of the same publication as Jones’ definition, Christoph A. Hafner offers a definition of digital identity that directly contradicts both Jones’ and Bratton’s data-driven self. Hafner instead defines digital identity as a ‘second-self,’ a performative avatar that a user iterates over, making changes to the content of the identity during its lifetime: *“As with other online spaces, virtual worlds provide an opportunity for users to create a ‘second self’ (Turkle*

https://www.theverge.com/2024/6/3/24168733/zoom-ceo-ai-clones-digital-twins-videoconferencing-decoder-interview.

[163] Rodney H. Jones, “Discourse, Cybernetics and the Entextualisation of the Self,” in *Discourse and Digital Practices: Doing Discourse Analysis in the Digital Age*, ed. Rodney H. Jones, Alice Chik and Christoph A. Hafner (London: Routledge, 2015), https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781315726465-3.

[164] Benjamin H. Bratton, *The Stack: On Software and Sovereignty* (Cambridge, MA: MIT Press, 19 February 2016), https://mitpress.mit.edu/9780262029575/the-stack/ .

1985), with the potential to establish a 'fresh' identity (or set of identities) online. The conception of identity that is invoked here is informed by a sociocultural perspective, which sees identity not as a fixed, static entity but rather as something that is fluid and evolving."[165]

Although offered within the context of video games, this kind of definition can just as easily metastasise into policy initiatives: at the height of metaverse hype cultivated by incumbent technology companies in the early 2020s, the particular user-centric definition of identity offered by Hafner and others had a brief surge into the collective consciousness. Wholly incompatible with competing concepts of identity that demand cryptographic integrity and trust, the metaverse's version of digital identity nevertheless embraced by policy-makers at the European Commission in a short lived and ill-conceived 'Web 4.0' programme that promised to bring 'societal progress,' 'virtual public services' and a 'metaverse industrial ecosystem' to Europe.[166]

This is the grotesque circularity of the digital identity field: definitions are retrofitted to justify whatever technology venture capitalists are currently funding. The European Commission's embrace of metaverse identity: a concept that actively contradicts their own privacy legislation and exposes the intellectual shortcomings of institutional digital identity advocacy. Policy-makers do not seek coherent identity frameworks; they seek technological legitimacy for whatever Silicon Valley is selling this quarter.

~

As the wider world struggles with incompatible definitions of digital identity, this very conflict was represented directly within our qualitative participatory research. When prompted with the opening interview question, in which the researchers asked, *'What is your definition of digital identity?',* no two research participants provided a definition that could be described as aligned with another. Participants instead offered individualised definitions that, over the course of their interview, suggested strong influence from their occupations, their interests and political convictions:

"Digital identity is a way for me to prove who I am so that I can update or log into a product or service. I have an Apple ID that I got around 2002 and I have a whole host of

[165] Christoph A. Hafner, "Co-Constructing Identity in Virtual Worlds for Children," in *Discourse and Digital Practices: Doing Discourse Analysis in the Digital Age*, ed. Rodney H. Jones, Alice Chik and Christoph A. Hafner (London: Routledge, 2015), https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781315726465-7.

[166] European Commission, EU Strategy to Lead on Web 4.0 and Virtual Worlds (press release), 11 July 2023, https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition.

products and services associated with that, and now it has expanded to a family plan that includes my children and my ex-partner."

Research participant
Digital designer and researcher

"Digital identity is something that an individual controls that represents their digital persona from the individual standpoint. It can have as many characteristics as they deem necessary to define themselves in a digital context, like their name, date of birth, and other information."

Research participant
US-based healthcare data consultant

"Digital identities are leveraged in everything from presentational layers – like the positioning of oneself as an artist and assembling a performative identity that's legible online – to your passport. And also everything in between."

Research participant
Performer/composer and technologist

"To me, digital identity is the mechanism by which you gain access to digital resources, and the mechanism by which you grant access to digital resources. I do not consider that a complete definition, but at the end of the day, I think that is the operational definition that matters to most people: the idea that I gain access to systems and information and can grant access to the same."

Research participant
Open source activist in a leadership role

"This is one of those things that's really hard to overstate. I mean, digital identity is literally everything, right? Because if an attacker can adopt an identity, then there's no limit to what they can do."

Research participant
Cybersecurity consultant/former forensics investigator

"Digital identity is a gradient of assurance, it is not a singular concept or even context. It's a function of perception and requirements that starts with my innate self, that then is assessed against some other counterparty requirements. It's much easier for me to define what is not digital identity."

Research participant
Anti-fraud and risk management analyst

Participants working at a protocol level tended to incorporate technologies as part of their answer, and a participant's involvement in Web 2.0 and Web3 led them to name SAML/oAuth/etc, or tokens/wallets as part of their definition. Participants from theoretical or creative backgrounds tended to acknowledge the user-driven performative identity layer as key to digital identity, in stark contrast with participants from security backgrounds who described the curation and compartmentalisation of their identity as central to their own more paranoid or caution-driven definition of identity. Participants who identified as belonging to a vulnerable group or defined digital identity within colonial contexts provided definitions similar to security researchers, but tended to describe identity through the lens of corporate or state apparatuses.

~

'Digital identity' can thus be considered an umbrella term that describes both an abstract derivative and a forensically-sound representation of an individual, and everything in-between. Furthermore, the term refers to many parts of a digital system simultaneously; the presentational layer, the protocol (and its infrastructure), cryptographic primitives used to protect an identity or communication between two entities, or even the service providers accessed by a user. The immediate outcome of such a core ambiguity is a flattening of complex relationships between individuals into a simplified shorthand.

At the same time, the motivation to separate different layers of digital identity in pursuit of a universal definition creates new issues because those layers are enmeshed. In Problem Statement II, we described digital identity as a topology of power, while Problem Statement III highlighted their amorphous nature.

When pressed about the weaponisation of digital identity within the context of their professions, none of the participants who self-identified as proponents could offer substantial answers around the use of digital identity in statistically generated pre-crime profiles of real individuals. For participants working in industries where algorithmic pre-crime assessment is routine, such as healthcare fraud detection, employment screening, credit scoring, and border control, the refusal to acknowledge widly known weaponised applications is a worrying symptom that underlies the entire digital identity enterprise.

An individual's definition of digital identity is significantly influenced by external personal factors, such as socio-economic status, their background, their profession, and their own identity. Pressing participants to clarify their definition almost universally resulted in uncertainty, as irreconcilable idiosyncrasies and shortcomings inherent to digital identity introduced ambiguity in a participant's conceptual model. For example, participants working with digital identity in healthcare (either as a patient or a vendor) described digital identity in stark contrast to participants from civil society, and these differences covered infrastructure, public perceptions, privacy threats, implementation opportunities, scoping, classifications of identity, etc:

"That concept of digital patient identity is really a bit of a misnomer. To date it has not been defined in that same context [as citizen digital identity]. [...]

You know, if I'm receiving specific government services or programs that I'm leveraging my citizen digital identity to receive [specific government services], I don't think that's necessarily any less important than healthcare services. The origins of providing healthcare, the evolution of healthcare data around providing healthcare, have always created this sociocultural bastion where healthcare data is separate from everything else."

Research participant
Independent health IT consultant

Within the field, even clashing definitions are routinely folded into a single "first principle" of digital identity. A clear example is the boundary between state-issued and enterprise-issued credentials. Kim Cameron's seminal *Laws of Identity*, notes that the employment context is treated as an autonomous sphere, where staff generally expect credentials to be created and retired by their employer, not a government identifier that would expose day-to-day work activity to continuous state scrutiny:

"In many cultures, employers and employees would not feel comfortable using government identifiers to log in at work... the context of employment is sufficiently autonomous that it warrants its own identity, free from daily observation via a government-run technology."[167]

We found that these conceptual silos are rarely adhered to, even when intentionally accounted for by actors with the best intentions. Instead, identities designed to be encapsulated within a single use or specific relationship were rolled up and reused in other unintended contexts. Our interviews and literature review show this autonomy is often honoured in name only; over and over again, we documented examples – both with participants and in the wider field – where the boundaries of theoretical or practical intent

[167] Kim Cameron, The Laws of Identity, *Microsoft Corporation*, 12 May 2005, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

for a digital identity were overridden by opportunism or convenience. **In the absence of a universal definition of digital identity, everything becomes fair game. Identity is everywhere, and as a result, it is nowhere.**

~

Even partially-aligned definitions for digital identity revealed problematic and contradictory stances when examined closely. The concept of *trust* was an almost universally listed prerequisite for a digital identity system,[168] and this was seen both in the wider industry thinking and directly from research participants. But beyond the baseline inclusion of some kind of system of trust, the understanding of *what exactly trust is*, and what is considered trustworthy or not, diverges wildly between definitions.

Web3's definition of trust may be newer, but depends upon a conflicting pairing of trust; The protocol that governs the digital identity is designed to be *trustless*, an ungovernable or influence-free protocol utility enforced by cryptography nevertheless itself reliant on definitions of trust within the realm of information security.[169] Within the same techno-libertarian protocol design, identities must be capable of trust, and this definition is usually borrowed from asymmetric key exchange, where public keys represent a derived transaction address in a network-wide namespace.[170]

At the same time, proponents of so-called *web-of-trust*[171] digital identity systems claim that trust can designed for and cultivated within a digital identity system via a social graph. Two models are popular. A digital identity is held within an a reputable identity vendor, and the awareness of this custodianship within the wider world cultivates trust. Alternatively, a digital identity system is designed to be able to cryptographically sign other identities, creating a social graph that can be analysed to determine the trustworthiness (or not) of any identity in the network. Keybase, a PGP key management service, allowed users to cultivate trust by posting 'proofs,' cryptographic signatures published on a user's owned

[168] Lauren Yacono, "What Is Trust in Cybersecurity, and Why Can't We Assume It?" *Cimcor – State of Security* [blog], 20 July 2022, https://www.cimcor.com/blog/what-is-trust-and-why-cant-we-assume-it.

[169] Vitalik Buterin, "The Meaning of Decentralization," Medium, 6 February 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274; in outlining Web3's ethos, Buterin notes that blockchains create a "trustless" environment in which "participants can agree on the state of the system without having to trust any particular actor," shifting reliance from human institutions to openly auditable cryptography.

[170] Deloitte Insights, "In Us We Trust: Decentralised Architectures and Ecosystems," 6 December 2022, https://www.deloitte.com/us/en/insights/topics/technology-management/tech-trends/2023/trustless-blockchain-decentralized-internet.html.

[171] "Web of Trust," *Wikipedia*, last modified 19 June 2025, https://en.wikipedia.org/wiki/Web_of_trust. The Wikipedia definition of web of trust describes: "a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner," providing a decentralised alternative to certificate-authority-based PKI.

social media profiles, domain names, and other owned properties, creating a sort of almanac of identity through the ephemera of user-controlled digital presence.[172] We note, of course, that none of the incorporated trust-building third party systems were designed with this use case in mind.

At the centre of all issues of trust, little time is spent defining what *kind* of trust is at play. Trust itself shares many conceptual properties with identity, and possesses a multiplicity of definitions depending on the context of its use. Cybersecurity trust, for instance, is not at all the same as trust between economic actors: in cybersecurity, gaining the trust of the system is to be treated as a security breach.[173] But the digital identity industry profits from this confusion, deploying "trust" as a marketing term while building systems that systematically undermine every form of human trust that actually matters – trust in institutions, trust in privacy, trust in the possibility of authentic human connection.

Looking towards emergent identity-centric systems, this observation becomes stark. Web3's transactional (anti)trust model, where cryptographic verification replaces human relationship, represents the logical endpoint of this trajectory. What becomes critical is to introduce elements fundamentally at odds with this paradigm: definitions of trust that imply chains of reciprocity, care and agency between actors, rather than fraud, commodification and clientelism between parties of a transaction.

The endless invocation of "trusted digital identity," combined with a complete lack of standardisation and repeated catastrophic failure, cannot be seen as technical specification. The continued insistence towards trust[174] without acknowledging this central contradiction reveals advocacy rhetoric for what it truly is: a propaganda campaign designed to obscure the fundamental hostility of these systems to the social bonds they claim to protect.[175] At the core of this phenomena is the inability to name it directly: this is made possible by the absence of a formalised definition of identity. ✳

[172] Keybase, "Keybase Proofs for Mastodon – And Everyone," *Keybase Blog*, 15 April 2019, https://keybase.io/blog/keybase-proofs-for-mastodon-and-everyone.

[173] Daniel Dobrygowski and William Hoffman, "We Need to Build Up 'Digital Trust' in Tech," *Wired*, 28 May 2019, https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech.

[174] Rachel Nyasani, Elena Gil and Saioa Echebarria, "Building Trust in the Digital Economy through Digital Identities," *techUK Insights*, 14 October 2024, https://www.techuk.org/resource/building-trust-in-the-digital-economy-through-digital-identities.html.

[175] Lily Hay Newman, "Aadhaar," in "The Worst Hacks of the Decade," *Wired*, 23 December 2019, https://www.wired.com/story/worst-hacks-of-the-decade.

2. Lack of industry and policy consensus creates gaps in accountability

Key Points

- No adversarial framework exists to test digital identity infrastructure before deployment, leaving critical flaws unaddressed.
- Ambiguity around accountability shifts responsibility onto users, who must act as identity managers without meaningful recourse.
- Utopian narratives like Estonia's digital state mask structural power imbalances and normalise state surveillance.
- Vendor and state accountability measures are often performative, failing to prevent systemic harm, as seen in Robodebt and Aadhaar.
- Biometric identity systems increase user risk while eroding legal protections and consumer rights.
- In practice, 'user sovereignty' means coerced compliance with service provider terms under threat of exclusion.
- Digital identity systems entrench inequality, undermine civic trust, and disempower both users and nation-states.
- Without genuine accountability, digital identity enables coercion, fraud, and systemic abuse at scale.

When digital technologies are implemented in societies, they reshape both power structures and the opportunities available through new digital systems. Digital identity systems, in particular, carry inherent ambiguities as unclear and often contradictory definitions, as well as weaknesses in their conceptual models and evaluations, which significantly influence their real-world outcomes. Within digital security, vulnerabilities are typically identified through adversarial security practices. These practices involve security experts acting as attackers to discover flaws in a system's design and implementation, detailing these vulnerabilities, and forecasting the potential consequences of exploitation. Proposed fixes are then typically tested through repeated adversarial analysis.

The need for cybersecurity is obvious. Yet, despite the explosive growth of the cybersecurity industry over the last twenty years, there remains no equivalent adversarial socio-technical security practice to analyse digital infrastructure *before* it is implemented. Consequently, deeper conceptual flaws beyond cybersecurity's immediate scope often remain unchallenged and unaddressed.[176] This gap is particularly dangerous given that digital identity itself lacks a coherent, universally accepted definition, as detailed in our first finding. This definitional ambiguity is not merely academic; it enables specific mechanisms that create accountability vacuums. These mechanisms include **the obfuscation of responsibility through algorithmic decision-making**, **the shifting of legal burdens onto individuals through consent-based models of 'user sovereignty'**, and **the creation of centralised points of failure**

[176] Christopher Allen, "Echoes from History II: The Dangers of eIDAS," *Blockchain Commons*, 21 November 2023, https://www.blockchaincommons.com/articles/eidas/.

that amplify the potential for fraud and abuse. In the context of digital identity systems, these oversights have severe implications. The most tangible effects of these accountability gaps include shifting responsibility from providers to users, appointing individuals as involuntary identity managers, and limiting citizens' ability to negotiate equitably with identity or service providers. As policymakers and technology vendors continue to communicate ineffectively, these fundamental socio-economic and legislative consequences remain unresolved.

~

In an August 2020 keynote, Estonian President Kersti Kaljulaid described digital identity as foundational for social cohesion within a connected society: *"How can you ask people to apply proper cyber hygiene, if they do not have a way to identify themselves to each other while they act and transact online? Everything starts from governments, who are the only entities, who have the legal space control, who can actually create digital identities, which are respected by all parties and they should work internationally."*[177]

Estonia's computer-addicted government has spent twenty years arguing the case for a mandated state digital identity both at home and abroad. Digital identity proponents have positioned Estonia's scheme as the only means to efficiently govern a complex modern society. Years after helming the digitisation of Estonia's government and financial sector, Toomas Hendrik Ilves stood before the UN and positioned Estonia's 2012 digital election as a success: *"Twenty-one years after restoring our independence, Estonia is an example where a combination of responsible free enterprise, E-governance, international partnerships and eco-friendly policies can put you in the fast lane of development. [...] [Estonia's digitised public service] has increased the possibility to exercise fundamental rights and freedoms and improve inclusive and responsible governance."*[178]

This utopian advocacy for the digitised society is not new and not unique to Estonia, but the country's early and successful implementation of a national identity scheme includes then-novel fundamentals that have subsequently been adopted and normalised throughout the world. Within Estonia's digital society, citizens are able to transact with the government in highly personal contexts, such as medical care and prescription refills, participating in an election, or enrolling their children into childcare and schooling services. In all cases, this is presented as effortless and secure despite a tremendous amount of data generated and

[177] Kersti Kaljulaid, "Opening address, Latitude 59 conference, Tallinn", *YouTube*, 2020, https://www.youtube.com/watch?v=ExdNDfYA6Jg.

[178] United Nations, "Information Technology Can Transform Countries, Estonian President Tells UN Debate," *UN News*, 26 September 2012, https://news.un.org/en/story/2012/09/421232.

stored on citizens with each transactions. However, despite their conceptual aspirations of user empowerment, efficiency, innovation or transparency, these fundamentals create significant reconfigurations of power relations between users, service providers and identity providers.

To combat criticisms of surveillance, Ilves' digitisation office proposed the concepts of *state accountability*, where state workers are surveilled while accessing stored data on citizens and disciplined for improper use, and so-called *user data sovereignty*, where the citizen is designated with the the responsibility to set and manage individual access rights of their personal information for service providers.[179] Although widely marketed as a set of policy and systems innovations, these two concepts are an acknowledgement of the inescapable surveillance capabilities of a digital state, made possible by combining the promises of frictionless access to citizen records and the implementation of an all-encompassing and data-rich digital identity. Having been unable to cryptographically prevent the weaponised design[180] potential inherent in such a system, the proposed solutions are instead *socio-technical*, where the acknowledged interplay between state as an identity vendor, service providers, and users produce emergent threats wholly beyond the system itself.[181]

It goes without saying that *vendor accountability* is an unconvincing policy whose enforcement remains subject to the discretion of relevant authorities. One prominent example is the Australian government's Robodebt scheme, a bipartisan[182] [183] digital identity system intended to algorithmically eliminate welfare fraud. Ironically, the system itself unlawfully.[184] issued hundreds of thousands of debt notices based on flawed algorithms without adequate proof.

Between July 2016 and October 2018 alone, data from the Department of Human Services revealed that 2,030 people died after receiving a Robodebt notice, with nearly a third of them classified as "vulnerable." The scheme inflicted significant financial distress,

[179] Kersti Kaljulaid, "President of Estonia: How Do We Improve Security and E-Governance?" *e-Estonia*, 8 September 2016, https://e-estonia.com/president-of-estonia-how-do-we-improve-security-and-e-governance/.

[180] Cade Diehm, "On Weaponised Design," Our Data Our Selves, *Tactical Tech*, 16 February 2018, https://newdesigncongress.org/en/pub/on-weaponised-design.

[181] Matt Goerzen, Elizabeth Anne Watkins and Gabrielle Lim, "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework," *9th USENIX Workshop on Free and Open Communications on the Internet* [FOCI '19], Santa Clara, CA, 14 August 2019, https://www.usenix.org/conference/foci19/presentation/goerzen.

[182] Chirrag Shah, "Australia's Robodebt Scheme: A Tragic Case of Public-Policy Failure," *Blavatnik School of Government Blog*, 26 July 2023, http://www.bsg.ox.ac.uk/blog/australias-robodebt-scheme-tragic-case-public-policy-failure.

[183] Josh Adams, "Labor Falls Short on Robodebt Royal Commission Measures," *Green Left*, 5 December 2023, https://www.greenleft.org.au/content/labor-falls-short-robodebt-royal-commission-measures.

[184] Human Rights Law Centre, *"The Federal Court Approves a $112 Million Settlement for the Failures of the Robodebt System,"* 11 June 2021, https://www.hrlc.org.au/human-rights-case-summaries/2021/9/30/the-federal-court-approves-a-112-million-settlement-for-the-failures-of-the-robodebt-system.

emotional trauma, and resulted in several suicides.[185] Despite the harm, which led to a Royal Commission and the government being ordered to pay A$1.2 billion in a class-action settlement, no civil servant or government minister was held accountable, illustrating the systemic failure of accountability in digital governance.

Similar dynamics have emerged in Tanzania with the deployment of the National Identity Authority (NIDA). By 2021, nearly three-quarters of the eligible population had enrolled in Tanzania's national identity scheme.[186] However, systemic design flaws and insufficient legislative protections[187] created significant barriers to essential civic services. Citizens were forced into burdensome individual negotiations with service providers[188] and tasked with managing their own identity security.[189] These dynamics reinforced existing inequalities, leaving citizens vulnerable to exclusion with little accountability or avenues for redress.

The desire to deploy digital identity in democratic elections is another hallmark of accountability that, despite its flaws, remains unchallenged. Once again, Estonia's digital state is considered a pioneer of electronic and internet-based voting and governance,[190] however, a 2014 study by an international team of security researchers identified critical social engineering and 'false verification' attacks, rendering vote casting systems vulnerable to real-time manipulation.[191] In a damning disclosure, the researchers warned that the flaws were so deeply rooted in the voting system's architecture, that the only correct course of

[185] Mark Dreyfus, "After Robodebt: Restoring Trust in Government Integrity and Accountability," *The Monthly*, 1 February 2024, https://www.themonthly.com.au/issue/2024/february/mark-dreyfus/after-robodebt-restoring-trust-government-integrity-and.

[186] National Audit Office of Tanzania. *Registration and Issuance of National Identification Cards to All Eligible Citizens: Performance Audit Report*. Dodoma, March 2021. https://www.nao.go.tz/uploads/Registration_and_Issuance_of_National_Identification_Cards_by_NIDA.pdf.

[187] Patricia Boshe, "Tanzania: NIDA IDs for Civic Services, or Not?" *Research ICT Africa* [blog], 16 July 2021, https://researchictafrica.net/2021/07/16/tanzania-nida-ids-for-civic-services-or-not/; Boshe notes that "as of March 2021, 18.7 million people – about 74 percent of the eligible population – had received their NIN," yet many were still "locked out of SIMs and mobile-money services" unless they negotiated directly with providers to synchronise biometrics with the NIDA database.

[188] Mussa Juma, "Legal Confusion as Millions of SIM Cards Blocked," *The Citizen*, 21 January 2020. https://www.thecitizen.co.tz/tanzania/news/national/-legal-confusion-as-millions-of-sim-cards-blocked-2701766.

[189] Patricia Boshe, Digital Identity in Tanzania: Case Study Conducted as Part of a Ten-Country Exploration of Socio-Digital ID Systems in Parts of Africa, *Centre for Internet & Society*, 31 October 2021, 46-48, https://africaportal.org/wp-content/uploads/2023/06/Tanzania_31.10.21-1.pdf; of note, the report highlights systemic design flaws: "no data-protection authority, no clear redress mechanisms, and obsolete legislation dating to 1986" – that leave citizens "responsible for safeguarding their own identities" and vulnerable to exclusion from essential services.

[190] European Commission, *Estonia 2024 Digital Decade Country Report*, 22 July 2024, https://digital-strategy.ec.europa.eu/en/factpages/estonia-2024-digital-decade-country-report.

[191] Lucian Constantin, "Estonian Electronic-Voting System Vulnerable to Attacks, Researchers Say," *PCWorld*, 12 May 2014, https://www.pcworld.com/article/439209/estonian-electronic-voting-system-vulnerable-to-attacks-researchers-say.html.

action was to discontinue internet-based voting until the system could be fundamentally re-engineered to prevent potential large-scale electoral fraud.[192]

The problem of democratic accountability extends beyond Estonia. For example, despite the attention around Estonia's digital civil society, the country is far from the first to host digital elections – India has relied on them since 1982,[193] adopting digitised electoral roll enrolment in 2023.[194] Proponents hail these systems as milestones in transparency for the world's largest democracy, yet India's electronic polling has continually faced calls for full reconciliation of electronic tallies with paper verifications.[195]

In many cases, those demands remain unmet, casting a deeply opaque digital shadow on suspected electoral fraud. On January 5, 2025, New Delhi Chief Minister Atishi publicly alleged a large-scale voter fraud scheme involving thousands of suspicious applications filed under names of individuals who denied submitting them, with local officials reportedly deleting records without proper verification.[196] This latest allegation is one of hundreds of real or suspected fraud within the country's e-voting systems, and comes after the Electoral Office spent the past five years linking voter rolls to India's national Aadhaar ID system, purportedly to combat electoral fraud.[197] In a recent Mumbai rally, Congress Party leader Rahul Gandhi went so far as to assert that Prime Minister Narendra Modi "can't win polls without EVMs, ED, CBI, and I-T,"[198] accusing the ruling party of undermining democratic institutions via relying on compromised voting infrastructure.

~

While the concept of *user data sovereignty* is widespread and often described as users having control over their own data, this control is effectively ceded the instant the data is

[192] Drew Springall et al., "Security Analysis of the Estonian Internet-Voting System," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security [CCS '14]*, 703–715 [New York: ACM, 2014], https://doi.org/10.1145/2660267.2660315.

[193] Pallava Bagla, "'Pioneer of Digital Democracy': India First Country in the World to Use EVMs," *NDTV*, 17 May 2024, https://www.ndtv.com/india-news/lok-sabha-elections-2024-india-1st-country-in-the-world-to-use-evms-5684833.

[194] Anjan Pathak, "From EVMs to Blockchain: How Technology Is Revolutionising India's Electoral Process," *BW Businessworld*, 3 June 2024, https://www.businessworld.in/article/from-evms-to-blockchain-how-technology-is-revolutionising-india%E2%80%99s-electoral-process-521914.

[195] Andy Mukherjee, "India's Voting Machines Are Raising Too Many Questions," *Bloomberg Opinion*, 11 April 2024, https://www.bloomberg.com/opinion/articles/2024-04-11/india-election-too-many-questions-loom-over-voting-machines.

[196] Arvind Kejriwal [@ArvindKejriwal], "Large Scale Fraud Taking Place in Voter Additions and Deletions in New Delhi Assembly …," *=X*, 6 January 2025, https://x.com/ArvindKejriwal/status/1876231055763804579.

[197] Vikaspedia, "Link Your Aadhaar and EPIC | Digital Governance," accessed 4 April 2025, https://egovernance.vikaspedia.in/viewcontent/e-governance/online-citizen-services/government-to-citizen-services-g2c/all-about-aadhaar/link-your-aadhaar-and-epic?lgn=en.

[198] Purnima Sah and Abhinay Deshpande, "Modi Can't Win Polls without EVMs, ED, CBI, IT: Rahul Gandhi," *The Hindu*, 17 March 2024, https://www.thehindu.com/news/national/modi-cant-win-polls-without-evms-ed-cbi-rahul-gandhi/article67962220.ece.

transferred to the service provider. Service providers frequently make non-negotiable demands for personally identifiable information, insisting that users disclose sensitive data as a prerequisite for accessing their services.[199] If users refuse to comply with these demands, they are typically denied access, leaving them with little choice but to acquiesce if they wish to use the service. This undermines the stated aspiration of user sovereignty, as it strips users of meaningful control over their personal data once it is handed over. Instead of empowering users, the system reinforces the dominance of service providers who set unilateral terms, effectively eroding user agency through coercion and lack of post-interaction enforcement. The proposed solution, vendor accountability, is an idealistic appeal to power that highlights the inadequacy of user sovereignty in addressing these power disparities. When a digital identity is deployed into a digitised society, it creates an opportunity to further centralise power away from users, and towards identity and service providers.

This combined power imbalance and vacuum of accountability is most prevalent in consumer finance, where the notion of user control over personal data is increasingly undermined. As part of broad anti-fraud efforts, banks continue to adopt newer forms of digital identity verification, including fingerprint scanning, facial recognition, and voice recognition.[200] The use of biometrics is positioned as essential for giving users more control over their identity and finances, yet they require users to surrender sensitive personal information. Once this biometric data is provided, control is effectively ceded. Regardless of whether the biometric is held by the user or even an fraud-detection third party, the power dynamic has shifted towards the user's non-negotiable surrender of sensitive information.[201]

At the same time, biometric technologies are used with increasing frequency to force customers to shoulder increasing financial risk. In instances of unauthorised transactions, banks have claimed that successful biometric verification is evidence that an account holder has approved a transaction, and subsequently refused to reimburse victims of fraud.[202] This effectively shifts the burden of proof onto the consumer, who must demonstrate that their immutable biometric data was somehow compromised — a daunting and often impossible

[199] Alexandra Giannopoulou, "Digital Identity Infrastructures: A Critical Approach to Self-Sovereign Identity," *Digital Society* 2, no. 2 (2023), https://doi.org/10.1007/s44206-023-00049-z.

[200] Anna Iwona Piotrowska, "Determinants of Consumer Adoption of Biometric Technologies in Mobile Financial Applications," *Economics and Business Review* 10, no. 1 (2024), https://doi.org/10.18559/ebr.2024.1.1019.

[201] L0la L33tz, "Banks Find AML 'Ineffective', Propose Access to Social Media," *The Rage*, 23 July 2024, https://www.therage.co/banks-aml-inefficient-access-to-social-media/.

[202] Joel R. McConvey, "Australian Bank Taps Facial Authentication Data to Challenge Disputed Transactions," *Biometric Update*, 22 July 2025, https://www.biometricupdate.com/202507/australian-bank-taps-facial-authentication-data-to-challenge-disputed-transactions.

task. In many jurisdictions, such claims are a flagrant disregard for existing consumer protection legislation, yet governments have been slow to address this behaviour. The implementation of biometric verification not only erodes consumer protections but also amplifies the existing power imbalance between service providers, users and the state. It underscores how the concept of user sovereignty fails to address these disparities, as users are compelled to relinquish control over their most personal data without genuine recourse or negotiation.[203]

~

In research interviews, participants described examples of how digital identities erode state or corporate accountability. The details varied widely, but shared common characteristics: digital identity became a *surface to project one's goals onto*, and the nature of this first principle could both obfuscate actors' intent and liability *and* allow for second-order consequences that leaves advocacy organisations, policy makers, or even citizens themselves racing to catch up. One participant, formerly employed to lead digitisation efforts within financial institutions, spoke openly about a culture that encouraged the development of user-centric identities through over-datafication and profiling, emboldened by a cavalier and dismissive culture around digital identity:

> *"What I saw was terrifying, a wild west with no rules. The goal of employees was to stay out of prison. Don't break any laws that you know about. Ask for forgiveness if you didn't know what you were doing was illegal. That culture keeps me up at night. It terrifies me. If we continue to create policy and regulation based off of what we have done for the past 20 years, it's going to be... actually, it's already a massive global problem. I think it's going to get even worse."*
>
> Research participant
> Corporate security researcher/former financial systems lead

Another participant, an academic and civil rights activist, described a similar void of accountability within the context of Aadhaar, a biometrics and demographics-derived mandatory digital identity scheme for India's 1.43 billion citizens.[204] [205]

[203] Ajinkya Kawale, "RBI Releases Draft Rules on AePS to Counter Frauds on Payments System," *Business Standard*, 31 July 2024, https://www.business-standard.com/finance/news/rbi-releases-draft-rules-on-aeps-to-counter-frauds-on-payments-system-124073101500_1.html.

[204] Unique Identification Authority of India, "Vision & Mission," *Government of India*, accessed 4 April 2025, https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india/vision-mission.html.

[205] Vikram K. Malkani, "Understanding Aadhaar, India's National Identification Initiative," *Indian Century Roundtable*, 13 September 2023, https://indiancentury.in/2023/09/13/understanding-aadhaar-indias-national-identification-initiative/.

> *"The government thought that the problem in the food subsidy programme was that, before I can go and withdraw my rations, you go and pretend to be me and take my rations. And so, they proposed to use biometric authentication [Aadhaar] to ensure that only I can get my ration and not you.*
>
> *Where this technology is supposed to stop fraud, it actually ends up empowering corruption within the bureaucracy. The authority responsible for distributing food subsidies checks my Aadhaar identity and tells me, 'Oh, the authentication has failed.' But in fact, it's gone through. The fraud point is centralised and lucrative, and Aadhaar makes this possible. Instead of holding fraudulent operators accountable, the entire population is being punished with this crazy technology and being made to pay the price for somebody else's faults."*

Research participant
Academic and civil rights activist

The data paints an even bleaker picture. While Aadhaar has reached over 1.2 billion enrolments and is linked to over 1,600 government schemes, its implementation has been plagued with issues. A 2019 study by Dalberg found that while many users reported benefits, 0.8% of people were denied essential services like food rations due to Aadhaar-related failures, affecting millions.[206] The same study noted that marginalised groups, such as homeless and transgender people, have significantly lower enrolment rates (30% and 27% respectively lack Aadhaar). This exclusion from the foundational ID system effectively bars them from critical welfare.[207]

This criticism is not specific to Aadhaar. Instead, it illustrates how the use of digital identity as an enforcer of accountability creates a new set of ambiguities that remain unaccounted for, such as when "ration shop owners were asked to take photographs of [people for whom fingerprint authentication failed] before giving them food rations"[208] or when the UIDAI failed to file "a single case against anyone" as a result of the 'Aadhaar leaks' scandal (in theory "punishable by up to three years in prison").[209] In the case of the various welfare programmes in India, where bureaucratic failures and corruption is well documented.[210] Here, recipients now navigate an apparatus whose corruption is centralised and

[206] Swetha Totapally et al., *State of Aadhaar Report 2019*, Dalberg, 2019, https://dalberg.com/wp-content/uploads/2025/06/State-of-Aadhaar_2019_Report_web.pdf.

[207] Arya Raje and Ganesh Pandey, "Unseen and Unrecognised: The Indians Excluded from Aadhaar," *Haqdarshak*, 24 August 2023, https://haqdarshak.com/2023/08/24/unseen-and-unrecognised-the-indians-excluded-from-aadhaar/.

[208] Dissent on Aadhaar: Big Data Meets Big Brother, ed. Reetika Khera [Hyderabad: Orient BlackSwan, 2019].

[209] Ibid.

[210] Ibid.

emboldened by a new impunity made possible by the system's design. At the same time, within the same system, these citizens have lost the ability to negotiate with the state.

Over time, the potential consequences of digital identity on power relations have become more widely understood and led to a rising resistance to digital. In 2019, following the World Food Programme's biometric and blockchain powered Building Blocks pilot project in Jordan two years earlier, Houthi authorities resisted attempts at "ventriloquis[ing] for the poor,"[211] protesting the deployment of similar schemes within Yemen and [identifying the central role biometric digital identity plays in challenging local sovereignty.[212] As a result, the final design of the aid project granted Houthi control over data storage and access – a decision by the World Food Programme that may have its own unforeseen consequences.

In Western contexts, humanitarian or crisis based identity systems follow a similar trajectory, shifting the burden of proof from identity and service providers to individual users. In *Digital identity as platform-mediated surveillance*, Silvia Masiero highlights the case of the "shift in the Eurodac system, which univocally identifies asylum seekers in European countries through their fingerprints, in 2015 made the Eurodac database interoperable with national police authority databases across Europe."[213] In the US, medical

[211] Keith Breckenridge, "Lineaments of Biopower: The Bureaucratic and Technological Paradoxes of Aadhaar," *South Asia: Journal of South Asian Studies* 42, no. 3 (2019), https://doi.org/10.1080/00856401.2019.1613080.

[212] Aaron Martin et al., "Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions," *Geopolitics* 28, no. 3 (2023), https://doi.org/10.1080/14650045.2022.2047468.

[213] Silvia Masiero, "Digital Identity as Platform-Mediated Surveillance," *Big Data & Society* 10, no. 1 (2023), https://doi.org/10.1177/20539517221135176.

records from abortion clinics and client data from domestic violence organisations are routinely used by immigration enforcement officers during dragnet operations targeting suspected undocumented migrants,[214] and often the integrity or accuracy of such policing operations remains completely unchecked.[215] In this case, even a heavy regulatory effort targeting digital identity would fail to address the core problem: it is difficult to argue than even a plurality of users of abortion clinics would wish to carry this digital identity and corresponding medical data as an attribute in a centralised wallet, or in a decentralised one held onto a device easily stolen or seized. Instead, the only path forward that avoids such abuses is to fully anonymise and segregate the data beyond the reach of any digital identity. This is at odds with the desires of digital identity proponents, particularly those who embrace the Ilves-style rhetoric of the responsible, all-knowing, digitised social state.

~

Finally, digital identity erodes state sovereignty itself. Operating through a radical redistribution of responsibilities between institutions, the shifts in accountability created by the deployment of digital identity controlled by third parties parallels the disempowerment born from the loss of control over other forms of infrastructure through privatisation. The 20th century is filled with examples of the erosion of state stability and social cohesion through rampant privatisation. In the modern digitised society, the control of underlying infrastructure for which a digital system is built on top of is of equal importance, but rarely included in analysis of state digital sovereignty. This has immediate consequences.

Since 2022, Ukraine has relied on Starlink for satellite internet for citizens and defence, and this dependency has been leveraged against the state by Elon Musk.[216] In Brussels, the dream of the smartphone-based European digital identity (eIDAS) will have to rely heavily on Amazon AWS servers[217] and the Apple and Google smartphone duopoly, creating a sovereign dependency on foreign companies that are regularly sued by European regulators.

Everywhere digital identity is deployed, complex questions around sovereignty and accountability are raised. In response to each new wave of systemic failure, new regulatory

[214] Dhruv Mehrotra, "ICE Is Grabbing Data from Schools and Abortion Clinics," *Wired*, 3 April 2023, https://www.wired.com/story/ice-1509-custom-summons/.

[215] Olivia Empson, "IRS Nears Deal with ICE to Share Data of Undocumented Immigrants – Report," *The Guardian*, 23 March 2025, https://www.theguardian.com/us-news/2025/mar/23/irs-ice-deal-share-data-undocumented-immigrants.

[216] David Klepper and Lisa Mascaro, "Here's a Look at Musk's Contact with Putin and Why It Matters," *AP News*, 25 October 2024, https://apnews.com/article/musk-putin-x-trump-tesla-election-russia-9cecb7cb0f23ccce49336771280ae179.

[217] Borja Larrumbide and Daniel Fuertes, "Customer Checklist for eIDAS Regulation Now Available," *AWS Security Blog*, 9 May 2023, https://aws.amazon.com/blogs/security/customer-checklist-for-eidas-regulation-now-available/.

frameworks and technical standards are invariably proposed as definitive solutions. Yet these proposals often arise from the same misguided thinking and flawed first principles that created the initial problems, promising user control and security while reinforcing the very power imbalances they claim to solve.[218] This cycle of failure, followed by promises of a technical or legislative fix, serves to obscure the fundamental nature of the problem.

Everywhere digital identity is deployed, complex questions around sovereignty and accountability are raised. Our research shows that these complex dynamics around legitimacy, control, power and care continue to be ignored by most, if not all, actors in the field.

Such accountability failures remain unresolved, even in emerging policy and technical specifications. A recent technical analysis of the eIDAS network found that, in practice, many solutions fail to follow modern security guidelines because *"solution providers trade security for simplicity."*[219] In other words, regardless of the technology or the motivations of their designers: *there is yet to exist a frameworks that is capable of eliminating the core issues of power imbalance and the potential for systemic harm, enabled by digital identity systems.* Our research shows the opposite, that these complex dynamics around legitimacy, control, power and care act as a disconnect, creating hidden accountability gaps that allow their most egregious failures be ignored by most, if not all, actors in the field. ✳

[218] Christoph Schmon, Marta Staskiewicz and Théa Hallak, "eIDAS 2.0 Sets a Dangerous Precedent for Web Security," *Electronic Frontier Foundation Deeplinks Blog*, 5 December 2022, https://www.eff.org/deeplinks/2022/12/eidas-20-sets-dangerous-precedent-web-security.

[219] Marko Hölbl, Boštjan Kežmah and Marko Kompara, "eIDAS Interoperability and Cross-Border Compliance Issues," *Mathematics* 11, no. 2 (2023), https://doi.org/10.3390/math11020430.

3. Authentication-centric models are out of step with how people build trust

> *“To prove digital identity, practitioners now explore biometrics – whether it’s an iris scan, a fingerprint, your DNA or some kind of proprietary or novel data point. I don’t think these approaches work that well. Conceptually, these aren’t our identity. We live in a social construct. If someone puts their hand up and identifies themselves as me, we go to an authority that has the final say on who I am. I often think about how that dispute would be resolved, what would be the methodology used to determine who is me, and who is not? Despite the procedures and the tactics deployed by this authority, the intent of all that work boils down to social consensus.”*
>
> Research participant
> Anti-fraud and Risk Management Analyst

As the international community continues its struggle to secure the ever entangling web of networks it has built, the social, economic, and more recent political damage caused by successful social engineering attacks continues to accelerate, both in scope and impact. This research finds that despite an expensive multi-decade effort to harden the world’s networks,[220] such work has failed to curtail ever-effective social engineering attacks.[221] We argue this is caused by a conceptual ubiquity in systems design: Almost all implementations of digital identity combine the Authentication and Presentation properties into one entity, creating an *‘I authenticate, therefore I am’* strategy that is odds with how human societies cultivate identity and trust outside of digital systems. We believe that, given that social engineering continues[222] to be an exponentially growing issue,[223] this clash

Key Points

- Dominant digital identity models centre on authentication, collapsing access and recognition into a single mechanism: *I authenticate, therefore I am.*
- This Cartesian logic is misaligned with how humans build trust through non digital contexts.
- Such systems ignore ambiguity and nuance, which are exploitable openings for social engineering and identity fraud.
- Post-colonial and relational critiques show identity is co-constructed, context-sensitive, and cannot be reduced to fixed attributes.
- Digital identity systems hardcode power asymmetries by treating mutable, lived identities as static, verified data.
- Without separating authentication from recognition, identity remains vulnerable.

[220] Ken Withee and John Flores, “Microsoft Cybersecurity Defence Operations Center,” *Microsoft*, 12 March 2025, https://learn.microsoft.com/en-us/security/engineering/fyl8-strategy-brief.

[221] Threat Research Team, Q2 / 2024 Threat Report, *Gen Digital*, 29 August 2024, https://www.gendigital.com/blog/insights/reports/q2-2024-threat-report.

[222] Roger Grimes, “If Social Engineering Accounts for Up to 90 % of Attacks, Why Is It Ignored?,” *LinkedIn*, 26 March 2024, https://www.linkedin.com/pulse/social-engineering-accounts-up-90-attacks-why-ignored-knowbe4-saeyc/.

[223] Verizon, *2022 Data Breach Investigations Report* [2022],

between social understanding of trust and the "Cartesian" nature of digital identity is the key vulnerability the makes such attacks possible. Our evidence for this can be found in the significant gaps between socio-biological methods for building trust and recognition – particularly in non-Western contexts – and analysis of key data breach reports and findings from interviews with research participants. Together, these observations suggest that, until alternatives to the Cartesian paradigm for digital identity are developed, it is likely that any future implementation of will remain critically vulnerable to social engineering.

~

In this key finding, as well as the problem statements previously this report, we describe the dominant and widely accepted conceptual implementation of digital identity as Cartesian in nature. We use this as a shorthand reference to *Cogito ergo sum*–"*I think therefore I am*"–one of Descartes' more well known claims that the individual self is found through conscious observation and rational thought. In other words, a person is a person through their ability to rationally observe the world and their own self.[224]

In the context of digital identity, the affirming claim *I think, therefore I am* applies almost literally. A digital identity, cultivated via processes of serialisation is leveraged by the user once they have provided credentials to access this constellation of identity markers, becoming *I authenticate, therefore I am.* The ability to provide credentials that match an identity provider is analogous to the ability to provide rational observations of the world, and therefore an individual's ability to demonstrate access, grants them unconditional representation of their self within the digital system.

I authenticate, therefore I am has evolved over time. In the era of Web 2.0, the over-reliance on user-generated content as a source for value extraction necessitated a parallel curation of the user's identity, specifically a presentational layer existing alongside authored content – *I curate, therefore I am.* Likewise, the subsequent financialisation of identity in the 2020s and the quantification of the self adds additional layers of economic language to the same underlying rationalist-based claim. This *"tendency of [liberalism] to confuse ontology with ownership (being with having)"* that we highlighted in Problem Statement II has fully coalesced into Web3's *I transact, therefore I am*. In this paradigm, digital identity proclaims a singular promise of KYC and cryptography backed user self-sovereignty, while deceptively turning the terms of the power equation on its head.

https://www.verizon.com/business/resources/reports/2022-data-breach-investigations-report-dbir.pdf.

[224] René Descartes, *Principia Philosophiae* (Amsterdam: Louis Elzevir, 1644).

The Cartesian approach to digital identity also sometimes claims that a user has sovereign agency over their identity. This is contradicted by the very nature of *"I authenticate, therefore I am."* No digital identity scheme truly allows users to exert their own wishes as to how they are identified, only to supply the attributes by which they will be identified (voluntarily or not) and that such attributes will be securely guarded and managed in novel way. The user self-sovereignty of digital identity stops firmly at baseline concerns for cybernetics, authenticity and cybersecurity; the most important facets for financial and commercial transactions, as well as questions of governementality. That is to say, in no way can you decide not to be identified by your gender, or your age, or your race if the scheme requires you to do so.

~

The Cartesian nature of digital identity is undeniably useful for systems design, and a core justification for cybersecurity itself. Cryptographic protocols and systems architectures typically adopt a binary logic that casts every entity either as part of the trusted "self" or as an adversarial "other" — a stance that echoes Descartes' own dualism in which external forces are treated much like deceptive demons attempting to obscure truth.[225] Descarte's rigid, paranoid clarity treats every outsider as potentially malevolent, and this worldview re-emerges through necesessity in cryptography as a means to ensure confidentiality is protected.

But this comes at a tremendous cost. Descartes' binary approach has been contested for centuries. Philosophers and scholars across multiple disciplines have long argued that identity cannot be reduced to fixed, mutually exclusive categories; rather, it emerges from complex, relational processes. In cybersecurity terms, clinging too tightly to such dichotomies risks overlooking the subtler forms of social engineering and insider threats that exploit ambiguities rather than clear-cut separations. It is also incomplete; The act of identity **serialisation** being a 'lossy' approximation of the iterative, citational, and disciplinary mechanisms through which humans verify each other, and how humans constitute and express identity. Combined, this unacknowledged flaw of ambiguity between the authentication and presentation layers of the Cartesian digital identity is the blueprint for social engineering.

Recent computer science scholarship especially has seen the emergence of post-colonial interrogation that challenges the Cartesian identity construct directly. Perhaps the most prominent example is Dr Abeba Birhane's work on Cartesian systems design and embracing

[225] René Descartes, *Principia Philosophiae* (Amsterdam: Louis Elzevir, 1644).

ambiguity in computing. In an essay entitled, *“Descartes was wrong: ‘a person is a person through other persons.”* Dr. Birhane argues that identity is fundamentally relational and context-dependent, shaped dynamically by interactions within diverse social contexts, such as friends, family, colleagues.

This is a relational understanding that stands in stark contrast to the rigid, immutable logic underpinning most digital identity systems: *“We know from everyday experience that a person is partly forged in the crucible of community. Relationships inform self-understanding. Who I am depends on many ‘others’: my family, my friends, my culture, my work colleagues. The self I take grocery shopping, say, differs in her actions and behaviours from the self that talks to my PhD supervisor. Even my most private and personal reflections are entangled with the perspectives and voices of different people, be it those who agree with me, those who criticise, or those who praise me.”*[226]

The demand for absolute certainty and control in digital spaces mirrors colonial registration practices, historically resisted by populations seeking autonomy from imposed official identities. Official registries never simply reflected reality, but instead often attempted to control it and existing in tension with informal, oral registers that communities utilised for authentic self-expression and autonomy. In describing the 20th century État-Civil in French Africa, Fredric Cooper wrote that: *“[...] officials were realizing that Africans were using état-civil in their own way, when they wanted it, for what they wanted. Registration of a birth for the sake of inscribing an official identity on the child was not the point, but when parents wanted the child to go to school, the alternative route to inscription had to be taken.”*[227]

Such registration efforts have had to coexist with popular acts of identification that could complete, modify, or challenge official acts. In what first appears to be an eerie parallel to Cooper’s testimony of civil unrest, Tamar Herzog writes of the identity governance efforts in early m Spain and Spanish America:

> *“Rather than constituting the person as the bearer of certain rights and duties, [identity documents and registries] indicated he may be thus. Rather than operating a transformation (making someone worthy of a certain treatment by the act of registering him or her), they recognized the validity of a change in status that had transpired beforehand, in fact sanctioning what oral negotiations had already consecrated. More*

[226] Dr. Abeba Birhane, “The Impossibility of Automating Ambiguity,” *Artificial Life* 27, no. 1 (June 11, 2021): 44–61, https://doi.org/10.1162/artl_a_00336.

[227] Frederick Cooper, “Voting, Welfare and Registration: The Strange Fate of the État-Civil in French Africa, 1945–1960,” in *Registration and Recognition: Documenting the Person in World History*, ed. Keith Breckenridge and Simon Szreter (Oxford: British Academy, 2012), https://doi.org/10.5871/bacad/9780197265314.003.0016.

often than not, rather than representing 'reality', registries gave proof of attempts by authorities [...] to control reality, attempts that were usually rejected [...]. [Written] registries always coexisted with an oral knowledge that either opposed or converged with them. How these two different registers coexisted (and perhaps coexist today) is a story we still need to explore."[228]

Dr. Birhane was writing about algorithmic automation and governance, but the removal of all doubt of the identity of a user is a necessary authentication, motivated by the broader goals of cybersecurity and data integrity. It is within this removal of doubt, and the excision of alternative registers, that the implied resulting absolute trust can be weaponised by an attacker through social engineering, something most humans struggle cognitively to counteract.

We believe the gap between Western epistemological assumptions and actual identity complexity is the unspoken root cause of the unsolved social engineering vulnerability that plagues digital identity. This gap is also precisely why all technical solutions to social engineering fail: they attempt to solve through more sophisticated authentication what requires entirely different approaches to recognition.

~

Regulatory responses to digital identity failures have doubled down on the very Cartesian assumptions that underlie systemic vulnerabilities. Standards like NIST's Digital Identity Guidelines (ISO/IEC 24760) and their accompanying Authenticator Assurance Levels operationalize a rigid, cryptographic model of *"I authenticate, therefore I am"* by enforcing technical specifications that privilege unassailable code over nuanced human trust-building practices.[229] In doing so, these frameworks reduce identity to a static set of attributes that remain Cartesian, and consequentually institutionalising a narrow conception of the digital self that ignores performative, relational dynamics.

This does not get better over time. Modern authentication protocols built on specifications like SAML and OAuth 2.0 strip away human judgment by abstracting verification into token exchanges;[230] valid tokens grant unconditional access even when contextual red flags

[228] Tamar Herzog, "Naming, Identifying and Authorising Movement in Early Modern Spain and Spanish America," in *Registration and Recognition: Documenting the Person in World History*, ed. Keith Breckenridge and Simon Szreter (Oxford: Oxford University Press, 2012), https://academic.oup.com/british-academy-scholarship-online/book/13503/chapter-abstract/167014682.

[229] Paul A. Grassi et al., *Digital Identity Guidelines* (NIST Special Publication 800-63-3, June 2017), https://pages.nist.gov/800-63-3/.

[230] Dick Hardt, *The OAuth 2.0 Authorisation Framework*, RFC 6749 (October 2012), https://tools.ietf.org/html/rfc6749.

exist, making compromised identity providers prime targets for social engineering. Biometric systems, especially government databases that treat physiological data as infallible proof, take this a step further: such technologies entrench the Cartesian digital identity by creating repositories of credentials that, once collected, are routinely targeted for theft. Decentralised alternatives such as the W3C's Decentralised Identifiers[231] (and other self sovereign models) to Vitalik Buterin's Soulbound token,[232] (and other Web3 models) simply replicate the same Cartesian logic. In all cases, an overreliance on cryptographic certainty distributes risk[233] rather than trust, sidelining the complex social relationships that might otherwise help detect impersonation or abuse.[234]

Recent synthetic media attacks demonstrate the consequences of the Cartesian digital identity, and the nihilism inherent how pervasive these problems truly are. The 2024 Hong Kong deepfake attack described in Problem Statement II was possible precisely because authentication verified "legitimate" participants through a digital identity. **What makes the Hong Kong attack so important, however, is that the attacker successfully tricked an employee by using a digital identity from *outside* the attacked system itself.** In other words, even when relying on humans as authenticators within predominantly digital systems, the incomplete nature of Cartesian digital identity remains a powerful vector. When a digital identity is inserted anywhere in the authentication stack, it immediately provides a powerful vulnerability to exploit, regardless of the ratio of human-to-machine verification within the system.

~

In research interviews, participants who engaged critically with the concept of *I authenticate, therefore I am* almost always acknowledged an unsatisfying gap between their **ideal identity** and the **flaws inherent to that ideal identity**. In many cases, participants could concretely point to examples of the absolute absence of doubt in digital identity authentication. Participants who identified as consultants or advocates with legal, cybersecurity or activist backgrounds offered countless stories of supporting victims of social engineering attacks that leveraged the digital identities of their loved ones or trusted corporations to trick, blackmail or coerce targets:

[231] World Wide Web Consortium, *Decentralised Identifiers (DIDs) v1.0* (W3C Recommendation, July 2022), https://www.w3.org/TR/did-core/.

[232] Vitalik Buterin, "Soulbound," blog post, 26 January 2022, https://vitalik.eth.limo/general/2022/01/26/soulbound.html.

[233] Bingqiao Luo, Zhen Zhang, Qian Wang and Anli Ke, "SoK: Anti-Fraud in Decentralised Finance," arXiv preprint, 30 August 2023, https://arxiv.org/abs/2308.15992.

[234] Cade Diehm, "This Is Fine: Optimism and Emergency in the P2P Network," *New Design Congress*, 16 July 2020, https://newdesigncongress.org/en/pub/this-is-fine/.

> *“We already have proof that our digital identities are tied up with our physical identities. In the US, a school shooter’s mother was convicted of manslaughter. A key piece of evidence that led to her conviction was that the mother had posted the gun on social media, and had written it was a Christmas present for her son [the perpetrator]. That’s an extreme example, but even so: How many times have I texted to my friend something that is friendly rivalry between us – ‘I’m going to kill myself’ or ‘I’m coming for you’! If somebody were to take a conversation, pluck it out of the blue, splice it here and here, it can pretty much make anybody sound awful because of my friends’ circle’s sarcasm. That’s what makes us ‘**us.**’ Who I am online is more than just what I put online, it is also how it is interpreted by the other party who knows me. I am a big proponent to make our own digital twins, of putting distance between our selves and our digital identity.”*

Research participant
Ph.D. Candidate, AI Researcher and Academic

These issues arise when the products of computer science are fused with the non-digital world. Some research participants highlighted profound legal implications arising from the Cartesian approach, directly or indirectly acknowledging that digital identities are increasingly legally tied to physical identities, with real-world consequences. One participant reflected:

> *“Authentication and and recognition are completely different. Authentication is a process of access, but recognition provides a presentational backbone to social interaction. They are linked, but they’re absolutely not the same. In many systems it is trivial to create a profile that mimics the user. I worry it will stay trivially easy even with new countermeasures.”*

Research participant
Cybersecurity consultant/former forensics investigator

Our interviews revealed a consistent struggle among participants to reconcile the theoretical promise of digital identity systems with their demonstrable vulnerability to manipulation and misuse. This was particularly true for participants in security or advocacy roles Participants frequently connected seemingly abstract authentication failures to tangible harms, illustrating how these technical shortcomings translate into real-world consequences for individuals and communities. The recurring theme across narratives is that effective digital trust requires a recognition framework grounded in human understanding, not one predicated on the flawed assumption of absolute certainty through cryptographic verification.

~

As highlighted in Problem Statement I and Problem Statement II, the exclusion of performative complexity creates exactly the vulnerabilities that social engineers exploit. Going further, our research shows that this **no current or emergent digital identity system has successfully countered this vulnerability.** This is why social engineering remains so devastatingly effective despite decades of cybersecurity investment. Attackers don't simply exploit technical vulnerabilities – they weaponise the performative gaps between lived identity and algorithmic recognition. The demand for absolute certainty and control in digital spaces mirrors colonial registration practices, historically resisted by populations seeking autonomy from imposed official identities. Official registries never simply reflected reality, but instead often attempted to control it and existing in tension with informal, oral registers that communities utilised for authentic self-expression and autonomy. The demand for absolute certainty and control in digital spaces mirrors colonial registration practices.[235]

What emerges clearly from these analyses is an urgent call to reconceptualise digital identity beyond its Cartesian origins. In the disruptive economic and security climate of 2025, the *"I authenticate, therefore I am"* model is increasingly weaponised, and increasingly exploited by bad actors, from deepfake-driven social engineering campaigns to authoritarian surveillance apparatuses such as the aggressive action of U.S. ICE agents. To effectively resist exploitation and reduce vulnerabilities, identity systems must accommodate complexity, relational dynamics, and social fluidity. This critical shift towards relational and consensus-based identity models could dramatically reshape digital security, making it inherently resistant to manipulation and better aligned with genuine human social experience. ✳

[235] Abeba Birhane, "The Impossibility of Automating Ambiguity," *Artificial Life 27*, no. 1, 11 June 2021, https://doi.org/10.1162/artl_a_00336.

4. Emerging technologies introduce new and potentially irreversible risks

"I understand you're putting all the safeguards in the world that you can imagine behind this, but if it gets compromised? What's the recourse? How does the person prove that it wasn't them behind the identity? There is no answer to that, and that's a huge problem for society."

Research participant
Ex-forensics investigator and cybersecurity consultant

Key Points

- Emerging technologies like biometrics, blockchain, and AI introduce lasting risks once embedded in infrastructure, often without recourse if compromised.
- Digital identity schemes use novelty to absorb the agendas of their surrounding political and cultural systems; they are never neutral.
- Biometric systems, rooted in carceral logics, were revived by surveillance demand and failing more often than claimed.
- Once deployed, identity tech reshapes societal power, reinforcing control and reducing individual agency.
- Technology always serves a moral and political project, whether acknowledged or not.
- The promise of precision gives way to degeneration at scale, turning tools of efficiency into instruments of coercion.
- Identity systems today are closer to 'disciplinary cyborgs' than emancipatory tools that conflate care with control.

Digital identity technologies marketed as "emerging,", including blockchain, biometrics, and artificial intelligence, carry inherent and substantial risks that often become irreversible once widely deployed. Our research demonstrates how these systems embed biases and governance structures at the protocol level, making correction computationally and politically difficult after implementation. The convergence of AI, biometrics, and blockchain in digital identity creates automated recognition systems that operate below the threshold of human oversight, transforming identification from a social process into a technical one with limited recourse mechanisms. The "emerging" label performs ideological work through novelty, reframing continuities with existing power structures as technological innovation while obscuring how these systems amplify rather than solve existing problems.

~

In 2025, digital identity finds itself firmly and indisputably enmeshed in the convergence of emergent technologies. Each arrives accompanied by its own liberation mythology: biometrics promises security, blockchain pledges decentralisation, AI offers objectivity. Yet each proves inseparable from the specific socio-technical projects that supported their development. Philosopher Yuk Hui's concept of *cosmotechnics* is instructive here: every technological system reflects the specific cosmological and moral framework in which it is developed. When applied to digital identity, Hui's philosophical project of "technodiversity" challenges the notion of a single, universal path for technological development. Hui argues that the dominant form of modern technology, originating in the West, should not be seen as the only form of technological thinking. Identity systems inherit and amplify the moral assumptions, institutional logics, and coercive tendencies of their origin. They are not neutral, conceived and built in a vacuum; they are expressions of authority. Hui's concept is critical in understanding why emerging digital identity technologies so reliably exacerbate existing societal and systemic vulnerabilities. The case of biometrics demonstrates the novel function of "emergence" perfectly. Biometric identification, aggressively marketed as an essential innovation for the past two decades, represents the triumphant return of Francis Galton's 19th-century eugenic classification projects, now optimised for digital processing speeds.

But as as Shoshana Amielle Magnet retells in her book *When Biometrics Fail*, the new, biometric-filled world we now live in is the tail-end of a 50-year long campaign of marketing and lobbying from a failing industry that had struggled to both find its purpose, and a viable market outside the prison industrial complex. Plagued by lack of access to compliant test subjects, important capital outlays, imperfect technology, and early discussion around data privacy, the biometrics industry remained moribund for decades, only saved by the crisis and perceived geopolitics risks arising after the attacks on the World Trade Center in 2001.[236]

Magnet's account is echoed by Bernard Dionysius Geoghegan's analysis of cybernetics: technologies that claim objectivity are in fact deeply shaped by the ideological frameworks of control and optimisation. Biometric systems, designed and tested under laboratory conditions, promise precision and trust—but degrade quickly in messy, contested, real-world contexts. At scale, they do not deliver clarity; they produce brittleness. They create systems that demand certainty in environments where uncertainty is the norm, punishing those who fail to conform.[237]

One of our participants, formerly a forensics investigator, put this in stark terms:

[236] Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham, NC: Duke University Press, 2011), http://www.dukeupress.edu/when-biometrics-fail.

[237] Silvia Masiero and Viktor Arvidsson, 'Degenerative Outcomes of Digital Identity Platforms for Development', *Information Systems Journal* 31, no. 6, 2021, https://onlinelibrary.wiley.com/doi/pdf/10.1111/isj.12351.

"I had a conversation with an EU researcher a few years ago. He was advocating for a biometric-based, government-issued digital identification. I asked him, 'I understand you're putting all the safeguards in the world that you can imagine behind this, but if it gets compromised? What's the recourse? How does the person prove that it wasn't them behind the identity?'

He had no answer for that. There is no answer to that, and that's a huge problem for society. Identity is the fundamental fabric to what's holding this all together, and if that breaks completely, it leaves us, essentially, in a trustless environment."

Research participant
Ex-forensics investigator and cybersecurity consultant

This failure is architectural. Biometric identity systems function as *disciplinary cyborgs*, to borrow David Lyon's term: devices that promise emancipation while embedding new regimes of control.[238] They frame the body not as an expressive agent, but as a database to be mined, a truth to be extracted, a problem to be managed. Lyon contrasts the liberatory promise of the cyborg – fluid, playful, transformative – with its disciplining reality: a system that bypasses consent in the name of certainty.

The history of fingerprinting centre around the act of recording a human's unique prints as an identity marker for later lookup. Fingerprinting provides a perfect early example of both the moral claim power imbued within the technics of identification, as well as their degeneration in enforcing existing power structures:

"Galton proved this hypothesis correct – that indeed fingerprints were unique and permanent, and quickly began a campaign advocating widespread use of fingerprints as a means of identification. From casting fingerprints as an external sign of heredity that could provide the underpinning for a program to cleanse the gene pool of bad stock, to viewing them as identifiers that would assure a place in jail for habitual criminals, was a small step for Galton. The notion of prevention and social control underlying both uses was the same: identify, sequester, control."[239]

While, historically, fingerprinting was an efficient way of distinguishing individuals inside police files, the technique coexisted with broader conceptions of criminality and morality. Here is cosmotechnics at play, in its most rudimentary form; The development of technics is

[238] Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Cambridge, UK Malden, MA: Polity, 2013).

[239] Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton, N.J: Princeton University Press, 2001).

geared towards the realisation of broader moral and societal order. Not much has changed over time.

~

For those in the digital identity landscape who are genuine about ethics and care, an inescapable complexity lingers. Just as our spheres of identity blur the conceptual lines between models, the notion of cosmotechnics highlights hanging and ambivalent effects of registration schemes. In *Documenting Individual Identity*, David Lyon provides a telling parable for digitised registration: that of the cyborg, at once liberating and policing:

> *“This is the other side of the coin, it seems, from the cyborg as a liberator, that allows playful transgression of old boundaries and the political potential to revise categories such as gender. [...] But such flexible representation stands in rather stark contrast with the design to tap into the body to obtain information untainted by the subject. This latter cyborg, it seems, is stripped of consciousness and the capacity to answer for herself, all in the paradoxical interests of accurate identification.”*[240]

In response to continued failures of digital identity, the next generation of emerging technologies propose the convergence of AI and biometric systems that bypasses human judgment entirely. Here, unlike in traditional biometric systems that require human verification, AI-powered facial recognition systems operate at a scale and speed that make human oversight impossible. Such technologies are already rolled out. Police departments from New York to Berlin to China to Dubai now deploy real-time facial recognition systems that can scan thousands of faces per second against databases containing millions of mugshots, generating automatic alerts without human intervention. The European Union’s Entry/Exit System processes biometric data from 700 million annual border crossings through fully automated AI analysis, making identification decisions that humans never review.[241]

This represents a qualitative shift from Lyon’s disciplinary cyborg to something more totalising: algorithmic identification that operates below the threshold of human perception or appeal. When these systems misidentify someone, the false positive becomes a machine-generated fact that can trigger arrest, deportation, or exclusion from services before any

[240] Ibid.

[241] European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), Entry/Exit System (EES) Annual Report 2023, *Publications Office of the European Union*, 2024, https://www.eulisa.europa.eu/sites/default/files/documents/consolidated-annual-activity-report-2023.pdf.

human becomes aware of the error.[242] The speed of algorithmic processing transforms biometric mistakes from correctable errors into irreversible events. This is cosmotechnics at its most coercive: an extenstion of the embedded moral assumptions into technology that is also capable of automating their enforcement at inhuman scales.

~

Digital identity is full of examples that fit the model of the cyborg, but perhaps the most astute of the emerging technologies is the blockchain. Despite apparent diversity via smart-contract platforms, layer-2 solutions, NFT identity systems, etc, these implementations share core assumptions about automated governance through protocol rather than democratic process, reproducing existing governance structures while claiming decentralisation. The trajectory from experimental technology to rapid appropriation by financial institutions, surveillance platforms, and state actors suggests how systems marketed as alternatives to centralised authority can concentrate power in fewer hands while making accountability more difficult to trace. From digital land titles to identity wallets, blockchain proponents promise identity solutions that shift verification from relational trust to automated protocol, encoding power not in people, but in code.

This is governance-by-smart contract, in which the political disappears behind infrastructure, offer a key insight to how cosmotechnics can be obscured by both rhetoric and technical infrastructures combined. David Golumbia argues in *The Politics of Bitcoin: Software as Right-Wing Extremism* that the liberatory rhetoric of bitcoin (and, thusly, the blockchain ledger itself) is a tool for imposing a policed structure on others.

> *"Bitcoin is not a politically neutral technology. It was developed explicitly to advance a very particular – and particularly radical – right-wing ideology. Its very structure encodes the belief that governments are inherently untrustworthy, that central banks are illegitimate, and that all forms of political regulation are obstacles to personal freedom. In this worldview, politics is to be replaced by protocol, and collective governance by cryptographic enforcement. Far from decentralising power, Bitcoin and blockchain technologies re-centralise it in the hands of those who write and maintain code – often unelected, unaccountable, and ideologically extreme."*[243]

[242] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81, 2018, https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[243] David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism, Forerunners: Ideas First from the University of Minnesota Press* (Minneapolis: University of Minnesota Press, 2016), https://www.upress.umn.edu/9781517901806/the-politics-of-bitcoin/.

Here again, the dream of precision gives way to degeneration at scale. This logic carries through directly to blockchain-based identity systems, where code enacts coercion under the guise of neutrality. Identity becomes programmable infrastructure—reconfigurable , by protocol enforcement that shreds any hope of participatory-consent. Governance, as Golumbia warns, is simply recast in the image of the developer. For Web3 identities, or certain implementations of biometrics, the blockchain's immutability becomes a trap that binds the identity to credential that cannot be revoked. There is no recourse for fraud, coercion, or simple human error, instead of decentralisation as freedom, what emerges is decentralisation as abandonment: governance without accountability, security without care.

Golumbia's more recent analysis in *Cyberlibertarianism: The Right-Wing Politics of Digital Technology* reveals that bitcoin is the prototype for a wider cyber-libertarian cosmotechnics.[244] He describes how "the power of math and cryptography" is supposed to supplant the levers of government, building a "new digital topography of trust" that disempowers democratic oversight while recentralising authority in the hands of those who control the codebase and computational resources.

In evaluating the infrastructure of digitised society, Golumbia observes: *"At its narrowest core, cyberlibertarianism is a commitment to the belief that digital technology is – or should be – beyond the oversight of democratic governments – meaning democratic political sovereignty. Frequently, the sentiment can be reduced to the view that democratic governments cannot or must not regulate the internet – or, to flip this formulation on its head, that the internet should be a place to which laws do not (or cannot) apply. Even in this narrow form, cyberlibertarianism is openly self-contradictory, alternating between the view that governments are unable to use laws to regulate digital technology and the view that governments must not be allowed to use laws in this way. These two ideas are incompatible."*[245]

But is Golumbia correct? To understand this, we take one more step back to events that unfolded over the duration of this research project. . In the run-up to Nayib Bukele's 2019 electoral victory in El Salvador, Bitcoin maximalists Max Keiser and Stacy Herbert raised campaign funds for Bukele in BTC.[246] [247] Following his victory, the Spanish newspaper El

[244] David Golumbia, *Cyberlibertarianism: The Right-Wing Politics of Digital Technology* (Minneapolis: University of Minnesota Press, 2024), https://www.upress.umn.edu/9781517918149/cyberlibertarianism/.

[245] David Golumbia, *Cyberlibertarianism: The Right-Wing Politics of Digital Technology* (Minneapolis: University of Minnesota Press, 2024), https://www.upress.umn.edu/9781517918149/cyberlibertarianism/.

[246] You're the Voice, "You're the Voice - Ep. 20: Max Keiser & Stacy Herbert - Bitcoin, Liberty & Hope," *YouTube*, 8 February 2024, https://www.youtube.com/watch?v=4Q37gekoOT8.

[247] John Knefel, "Tucker Carlson Guest Praises El Salvador's Authoritarian President for Failing Bitcoin

País *El País* reported that Keiser and Herbert were appointed by presidential decree to run El Salvador's "National Bitcoin Office," acting as gatekeepers for investors while designing public policy. Both are investors in Bitfinex/Tether and run crypto funds, giving them a financial stake in the very ecosystem they regulate.[248]

By 2021, those same donors engineered two large capital injections. First, stable-coin issuer Tether announced plans to move its headquarters to El Salvador after obtaining a digital-asset licence and negotiating tax holidays and regulatory carve-outs with Bukele's government. A *Reuters* report from January 2025 noted that Tether CEO Paolo Ardoino said executives would relocate and the firm would hire locally.[249] The report detailed that Tether's reserves are primarily held in U.S. Treasuries custodied by Howard Lutnick's brokerage Cantor Fitzgerald,[250] which *The Guardian* revealed holds a 5 percent stake in Tether and custodians most of its US$134 billion in reserves.[251]

Second, Reuters reported that half of a planned US$1 billion bond issue would be converted into bitcoin for the state's treasury, with the remainder funding infrastructure and bitcoin mining. Bitcoin evangelist and Blockstream chief strategist Samson Mow said these 10-year "Volcano Bonds" would pay 6.5 percent interest, with multiple issues envisaged.[252] This sale could potentially divert 50% of proceeds into Bukele's own Bitcoin treasury while bypassing the IMF.[253]

Within three months of the Tether deal, Bukele passed the Bitcoin Law, making the cryptocurrency legal tender and mandating every adult enrol in a biometric cryptocurrency wallet called *Chivo*.[254] An analysis by the James Madison Institute explains that while Article 7 compels "every economic agent" to accept bitcoin when offered, Article 12

Experiment," *Media Matters for America*, 1 December 2022, https://www.mediamatters.org/tucker-carlson/tucker-carlson-guest-praises-el-salvadors-authoritarian-president-failing-bitcoin.

[248] David Marcial Pérez, "Crypto evangelists enter the Bukele government: The dark business of bitcoin in El Salvador," *International*, 2 April 2023, https://english.elpais.com/international/2023-04-02/crypto-evangelists-enter-the-bukele-government-the-dark-business-of-bitcoin-in-el-salvador.html.

[249] Federico Maccioni, "Crypto firm Tether and its founders finalizing move to El Salvador," *Reuters*, 13 January 2025, https://www.reuters.com/technology/crypto-firm-tether-its-founders-finalising-move-el-salvador-2025-01-13/.

[250] Scott Melker, "Cantor Fitzgerald's Tether Ties Raise Concerns as Trump Nominates CEO for Commerce Secretary," *The Street*, 30 November 2024, https://www.thestreet.com/crypto/markets/cantor-fitzgeralds-tether-ties-raise-concerns-as-trump-nominates-ceo-for-commerce-secretary.

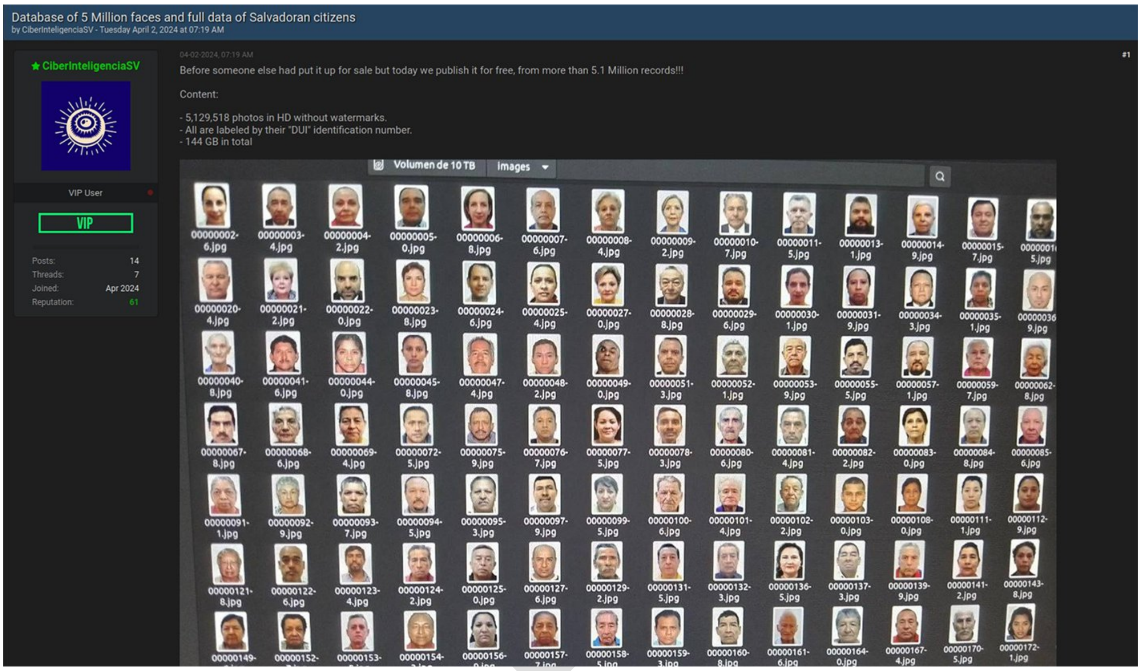
[251] Jason Wilson, "Trump cabinet member's links to El Salvador crypto firm under scrutiny," *The Guardian*, 14 May 2025, https://www.theguardian.com/us-news/2025/may/14/lutnick-el-salvador-crypto-immigration.

[252] Jonathan Laguán, "Meet Samson Mow, Architect of El Salvador's Bitcoin Bonds," *The Business of Business*, 22 March 2022, https://www.businessofbusiness.com/articles/meet-samson-mow-the-architect-of-el-salvadors-soon-to-debut-bitcoin-bonds/.

[253] Jessie Willms, "On the Ground in El Salvador with Samson Mow and the Volcano Bitcoin Bond," *Bitcoin Magazine*, 22 March 2022, https://bitcoinmagazine.com/markets/el-salvador-president-nayib-bukele-samson-mow-volcano-bitcoin-bond.

[254] Marcos Aleman, "El Salvador makes Bitcoin legal tender," *PBS News*, 9 June 2021, https://www.pbs.org/newshour/economy/el-salvador-makes-bitcoin-legal-tender.

exempts those without access to technology. The law does not force Salvadorans to hold bitcoin, and the government provided a public wallet.[255] Regardless, the Chivo wallet has already leaked 144 GB of personal data – a breach containing high-definition headshots and personal information (names, birth dates, addresses, and identity numbers) for more than 5.1 million Salvadorans. [256]


Database of 5 Million faces and full data of Salvadoran citizens
by CiberInteligenciaSV - Tuesday April 2, 2024 at 07:19 AM

★ CiberInteligenciaSV

VIP User

VIP

Posts: 14
Threads: 7
Joined: Apr 2024
Reputation: 61

04-02-2024, 07:19 AM

#1

Before someone else had put it up for sale but today we publish it for free, from more than 5.1 Million records!!!

Content:

- 5,129,518 photos in HD without watermarks.
- All are labeled by their "DUI" identification number.
- 144 GB in total

Figure: A screenshot from Breach Forums depicting part of the data dump of Salvadorian citizens, proportedly sourced from the Chivo mandatory bitcoin wallet.[257]

Simultaneously, security spending surged. Bukele broke ground on the 40,000-capacity CECOT megaprison in 2022.[258] This "Terrorism Confinement Centre" comprises eight concrete blocks where cells designed for more than 100 inmates have eighty bunks, minimal ventilation, and two toilets; At capacity, each prisoner would have only 0.6 square metres of space.[259] In the two years since its opening, human rights groups have tracked mounting deaths. A 2024 Cristosal report states that at least 265 detainees have died in Salvadoran

[255] Andrea O'Sullivan, "Reason: Is El Salvador's Embrace of Bitcoin Good, Bad, or Both?", *The James Madison Institute*, 6 July 2021, https://jamesmadison.org/is-el-salvadors-embrace-of-bitcoin-good-bad-or-both/.

[256] Helen Partz, "El Salvador: Hackers Leak Code of State Bitcoin Wallet," *Cointelegraph*, 23 April 2024, https://cointelegraph.com/news/el-salvador-hacks-leak-state-bitcoin-wallet.

[257] David Bernal, "Filtran base con datos personales de 5.1 millones de salvadoreños, tras no lograr venderlos en línea," *La Prensa Gráfica*, 6 April 2024, https://www.laprensagrafica.com/elsalvador/Filtran-base-con-datos-personales-de-5.1-millones-de-salvadorenos-tras-no-lograr-venderlos-en-linea-20240406-0021.html

[258] Devin B. Martinez, "CECOT: Bukele's Mega-Prison Where 'the Only Way Out Is in a Coffin'," *MR Online*, 22 April 2025, https://mronline.org/2025/04/22/cecot-bukeles-mega-prison-where-the-only-way-out-is-in-a-coffin/.

[259] Rhiannon Stevens, "What we know about CECOT, El Salvador's mega-prison taking Trump's deportees," *ABC News Australia*, 25 April 2025, https://www.abc.net.au/news/2025-04-26/cecot-mega-prison-trump-deportation-el-salvador/105200818

custody since the state of emergency began, amid conditions without light, hygiene, or access to food.[260] [261]

The same playbook was attempted with Argentina's libertarian President Javier Milei, ultimately a failed upstart of the right-wing crypto project. Milei rode a similar wave of anti-establishment crypto enthusiasm, promising to "obliterate" the central bank and mainstream Bitcoin. After Milei endorsed the $LIBRA token on social media, the token spiked then collapsed when eight wallets drained about US$99 million from its liquidity pool.[262] A federal judge opened an investigation into Milei's role, leading to lawsuits in New York and public interrogation in Argentina[263] over allegedly illicit association and fraud.[264] [265] Opposition politicians called for impeachment while the Argentine fintech chamber likened the episode to a "rug pull."[266]

Over half a decade, crypto's libertarian promise transformed into hard policy power in the United States. Industry PACs and dark-money groups spent more than US$130 million on the 2024 U.S. elections[267] and a further $10 million on Donald Trump's 2025 inaugural fund,[268] securing the first openly pro-crypto administration.[269] Within weeks, the newly-elected Trump administration invoked the Alien Enemies Act of 1798, re-labelled

[260] Amnesty International, "Unlawful Expulsions to El Salvador Endanger Lives amid Ongoing State of Emergency," 25 March 2025, https://www.amnesty.org/en/latest/news/2025/03/unlawful-expulsions-to-el-salvador-endanger-lives-amid-ongoing-state-of-emergency/.

[261] Pan Ho Liu, "Central America rights organization reports almost 80,000 arrests and over 250 deaths in El Salvador since 2022 state of emergency", JURIST News, 11 July 2024, https://www.jurist.org/news/2024/07/cristosal-reports-265-fatalities-79211-arrests-in-el-salvador-amid-state-of-emergency/

[262] Elizabeth Howcroft and Hannah Lang, "Crypto worth $99 million withdrawn from Milei-backed Libra token, researchers say," *Reuters*, 20 February, 2025, https://www.reuters.com/world/americas/crypto-worth-99-million-withdrawn-milei-backed-libra-token-researchers-say-2025-02-20/

[263] Nicolás Misculin and Lucinda Elliott, "Argentina federal judge to probe Milei crypto scandal, stock index falls," *Reuters*, 18 February 2025, https://www.reuters.com/world/americas/argentina-main-stock-index-falls-after-milei-crypto-scandal-2025-02-17/.

[264] Javier Lorca, "Milei, Acusado en Nueva York por la Cripto $Libra: 'Fue una Declaración Promocional Altamente Engañosa'," *El País*, 30 July 2025, https://elpais.com/argentina/2025-07-30/milei-acusado-en-nueva-york-por-la-cripto-libra-fue-una-declaracion-promocional-altamente-enganosa.html.

[265] Candelaria Schiappa-Pietra, "Milei's 'Iron Triangle' Creaks from the $Libra Cryptocurrency Scandal," *El País English*, 24 February 2025, https://english.elpais.com/international/2025-02-24/mileis-iron-triangle-creaks-from-the-libra-cryptocurrency-scandal.html.

[266] Harriet Barber, Javier Milei faces impeachment calls after Argentina cryptocurrency collapse, *The Guardian*, 17 February 2025, https://www.theguardian.com/world/2025/feb/17/argentinia-opposition-impeachment-milei-cryptocurrency-collapse.

[267] Jasper Goodman, "Crypto Won the 2024 Elections. Now Comes the Easy Part," *Politico*, 8 November 2024, https://www.politico.com/news/2024/11/08/crypto-2024-elections-00187415.

[268] Jasper Goodman, "Crypto Firms Pour Millions into Trump Inauguration," *Politico*, 17 January 2025, https://www.politico.com/news/2025/01/17/crypto-money-trump-inauguration-00199088.

[269] Danny Nelson, "Trump Becomes First Major-Party Candidate to Accept Crypto Donations," *CoinDesk*, 21 May 2024, https://www.coindesk.com/business/2024/05/21/trump-becomes-first-major-party-candidate-to-accept-crypto-donations.

Venezuela's Tren de Aragua as an "invasion force," and authorised the removal of "any alien or lawful permanent resident" linked to the gang, without notice or hearing.[270]

On 16 March 2025, amidst wider off-the-street kidnappings by masked and sometimes plainclothes ICE agents, a charter flight carried 238 Venezuelan asylum-seekers – most with no criminal convictions[271] – from Texas to El Salvador's CECOT mega-prison, where they subsequently disappeared.[272] U.S. Constitutional scholars note the proclamation's language sweeps in green-card holders, defying Supreme Court precedent that lawful permanent residents cannot be exiled without due-process safeguards.[273] In 2025, the same crypto-carceral machinery that targeted "foreign nationals" is now positioned to sweep up long-time U.S. residents via a digital-backed infrastructure with a documented growing list of detainee deaths and inhumane conditions.[274]

What's particularly chilling is how the narrative scaffolding operates: each component appears defensible in isolation; "Financial inclusion" through Bitcoin adoption, "public safety" through enhanced detention facilities, "innovation" through biometric wallets. Yet when examined together, the six-year Salvadoran story reveals crypto capture in its fullest expression, pieces interlocking into something far more sinister: a unified apparatus where cryptographic promises of liberation become the very infrastructure of globalised right-wing oppression.

Yuk Hui defines cosmotechnics as "the unification of the cosmic and moral order through technical activities." **El Salvador's Bitcoin experiment has crystallised a crypto-carceral cosmotechnics: Bitcoin-as-legal-tender, the biometric Chivo wallet, and the 40,000-inmate CECOT megaprison fuse code and corporeality in a single apparatus of control. To evaluate this infrastructure, and digital identity's pivotal role in sustaining it, is therefore to confront what Hui warns are the planetary stakes of allowing a single technological cosmology to eclipse all others: when**

[270] Donald J. Trump, "Invocation of the Alien Enemies Act Regarding the Invasion of the United States by Tren De Aragua," proclamation, 15 March 2025, *The White House*, https://www.whitehouse.gov/presidential-actions/2025/03/invocation-of-the-alien-enemies-act-regarding-the-invasion-of-the-united-states-by-tren-de-aragua/.

[271] Mica Rosenberg et al., "Trump administration knew most Venezuelans deported from Texas to a Salvadoran prison had no U.S. convictions," *The Texas Tribune*, 30 May 2025, https://www.texastribune.org/2025/05/30/trump-el-salvador-deportees-criminal-convictions-cecot-venezuela/.

[272] Human Rights Watch, "US/El Salvador: Venezuelan Deportees Forcibly Disappeared," 11 April 2025, https://www.hrw.org/news/2025/04/11/us/el-salvador-venezuelan-deportees-forcibly-disappeared.

[273] Congressional Research Service, "ArtI.S8.C18.8.7.2 Aliens in the United States," Constitution Annotated, n.d., accessed 30 July 2025, https://constitution.congress.gov/browse/essay/artI-S8-C18-8-7-2/ALDE_00001262/.

[274] Human Rights Watch, "El Salvador's Prisons Are No Place for US Deportees," 13 March 2025, https://www.hrw.org/news/2025/03/13/el-salvadors-prisons-are-no-place-us-deportees.

software is elevated to cosmic law, the most malevolent desires emerge as its material outcome.

~

The current models of digital identity turn personhood into programmable code. Such systems track who we are, determine what we can do, what rights we possess, and how we are recognised. The shift is subtle but total: identity – the representation of the individuals – is the core dependency, becoming the gateway for permissions, enforcement and coercion; A conditional access token modifiable at will. Infrastructural design becomes policy. Once deployed, these systems reshape the societies they were meant to serve.[275]

Once biometric databases exist, they do not vanish. Once blockchain credentials become infrastructure, they cannot be quietly retired. Once AI systems are trained on partial, biased data, they do not unlearn. These systems fossilise the assumptions baked into their design, making them difficult to question, harder to reform, and nearly impossible to dismantle. To believe these systems can be "fixed" without reckoning with their structural function is to mistake harm for friction. The history of fingerprinting was once sold as a tool for justice, but is now embedded in every border checkpoint and policing database, showing how quickly identification transforms into governance. Galton's eugenic logics remain encoded both historically and in the very technics of identity.

Everywhere emerging technologies are deployed in digital identity systems, they promise to solve the problems created by previous iterations while embedding the same fundamental flaws deeper into infrastructure. In response to each wave of systemic failure, new regulatory frameworks and technical standards are invariably proposed as definitive solutions. Yet these proposals invariably arise from the same cosmotechnical assumptions that created the initial problems, promising precision and objectivity while reinforcing the very power imbalances they claim to address. This cycle of failure, followed by promises of a technical fix, serves to obscure the fundamental nature of the problem.

Such failures remain unresolved even in emerging policy responses. The EU's AI Act attempts to regulate algorithmic bias through auditing requirements, yet these provisions cannot extract biases already fossilised in training data. New York City's Local Law 144 mandates algorithmic transparency in hiring, yet companies game the requirements by testing on narrow datasets that obscure real-world discrimination patterns. **There is yet to**

[275] David Golumbia, "The Critique of Cyberlibertarianism," *boundary* 2 51, no. 2, May 2024, https://read.dukeupress.edu/boundary-2/article-abstract/51/2/5/387538/the-critique-of-cyberlibertarianism.

exist a regulatory framework capable of addressing the core irreversibility problem embedded in emerging digital identity technologies.

To identify is to pre-empt, to assess, to control. **There is no neutral digital identity. And that means there is no technical fix for the current dominant cosmotechnics of digital infrastructure.** Our research shows that the most common outcome of the optimism promised by emergent, novel digital identity technology is almost always the opposite: that the convergence of AI, biometrics, and blockchain creates technological lock-in that operates below the threshold of democratic oversight, making resistance computationally impossible while claiming to deliver sovereignty and security to users. Without political resolve, cultural reckoning, and deliberate constraints on infrastructure, the convergence of 'emergent,' novel technologies, the cycle will repeat. Absent that reckoning, each new cycle will reproduce the same violences, only faster, cheaper, and with fewer means of resistance. ✳

5. Cryptographically secure identities complicate legal delegations

Today's digital identity systems underpin healthcare, finance, and democracy itself. Cryptography is widely adopted to combat social engineering, ensuring secure binding between individuals and their digital selves. Yet, paradoxically, our research demonstrates that cryptographically secured identities significantly flatten user agency, creating dangerous friction when delegation or third-party intervention becomes necessary.

Our research finds the security offered by the inclusion of cryptography in digital identity systems significantly flattens the structures of user control and agency. Two scenarios illustrate the severity of this issue clearly: intertwined identities such as familial or guardian relationships, and identities managed by a trusted third party. In scenarios critical to healthcare, social welfare, or involving marginalised groups, cryptographically rigid systems actively hinder effective third-party advocacy and legal delegation. Consequently, individuals are forced into unsafe, non-digital workarounds.

Key Points

› Cryptographic identity systems restrict legal delegation, complicating access in healthcare, family, and crisis contexts.

› One-device-one-user assumptions ignore shared-device realities, especially among vulnerable and marginalised groups.

› Secure identity design often conflates user with device, reinforcing control structures and enabling coercive dynamics.

› Legal exceptions, such as guardianship, power of attorney, or emergency care, require backdoors or workaround mechanisms, undermining core cryptographic guarantees.

› Zero-knowledge proofs deepen exclusivity without addressing the structural power behind identity requests.

› The rigidity of cryptographic identity risks becoming justification for backdoor mandates, whether by design or by law.

We believe that the contemporary political climate – where legislators from a number of Western countries have time and again sought to weaken end-to-end encryption for policing purposes – lays the groundwork for a clash clash between secure digital identity and the need for third party access to an individual's digital identity. This is an unexplored political issue that offers a compelling justification for the implementation of encryption backdoors to enable third-party access, and yet a proposal that must be resisted all the same.

~

As the digitised society reaches into increasingly sensitive and valuable areas of our lives, digital identity providers compete to design and implement cryptographically secure digital identity, leveraging advanced cryptographic methods to establish secure and unambiguous link between a digital identity and a single individual. Commonly associated with concepts such as self-sovereign identity, individual identity management of personal or financial data, or systems designed around families and other social relationships, the introduction of cryptography into digital identity systems promises to secure sensitive personal information and ensure that only the owner of a digital identity can use it to interact with service providers or provide access to data, thereby preventing forgery, impersonation, and unauthorised access or abuse.

In both the research case studies and wider landscape review, we identified specific sectors of digital infrastructure as responsible for leading the broader push to deploy secure implementations of digital identity: digital health records and patient care, operating systems (particularly those offered by Silicon Valley giants such as Apple and Google), financial sectors (particularly consumer finance), and state services where citizens interact with government. This observation was also present in the qualitative study phase of the research, and participants from a diverse range of professional or activist backgrounds overwhelmingly relied on these sectors to detail their observations around the strengths and shortcomings of secure digital identity.

While the wider adoption of secure digital identity has been propelled by specific sectors, the development of specific implementations of digital identity also have cryptographic requirements that influence cryptographically secure digital identity, both in design and practice. Web3, and other blockchain-based identity models almost always rely on a wider trustless environment, and enforce the use of immutable transaction histories that are forensically sound, in that they cannot be fraudulently modified or revoked by an adversary,[276] and pseudonymous, where they are generally agnostic to the identity of the parties involved in each transaction.[277] Despite the unproven nature of blockchain systems, their promise of user-sovereignty, and security in a wider chaotic digital space, has increasingly influenced the design and governance around digital identity. For example, the European Commission's eIDAS review, in examining the progress of the EU's implementation of its unified digital identity vision, has universally adopted both the lexicon of Web3 in its conceptualisation of the project, and consistently stresses a cryptographically secure implementation of digital identity in a wider trustless world:

[276] Hany F. Atlam, Ndifon Ekuri, Muhammad Ajmal Azad, and Harjinder Singh Lallie, 'Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions,' *Electronics* 13, no. 17, 8 September 2024, https://doi.org/10.3390/electronics13173568.

[277] Nitish Andola, Raghav, Vijay Kumar Yadav, S. Venkatesan, and Shekhar Verma, 'Anonymity on Blockchain Based E-Cash Protocols-A Survey,' *Computer Science Review* 40, 1 May 2021, https://doi.org/10.1016/j.cosrev.2021.100394.

“Member States shall ensure that the set of person identification data attributes issued to a given wallet user is unique.”[278]

“Wallet providers shall ensure that [...] the wallet secure cryptographic application has authenticated the identity of the wallet user.”

“[...] providers shall ensure that wallet units authenticate and validate wallet using only the trusted list of providers of wallet party access certificates referred to in Article 18 of Implementing Regulation” [279] [280]

~

To understand how secure digital identity affects digitised societies and threatens cryptography policy itself, we must first revisit some of the basics of cryptography. Public key encryption is a information security primitive that involves each party possessing a unique pair of cryptographic keys: a public key and a private key. When Alice wishes to send a secure message to Bob, she encrypts the message using Bob’s publicly available public key. Only Bob, holding the corresponding private key, can decrypt this message, ensuring confidentiality and security.[281]

Public key encryption is a fundamental information security paradigm and a common dependency for the design of digital identity. At its core, this design invokes a unique association between each user and their cryptographic key pair. While Alice and Bob are identified as individuals, the cryptographic operations are performed using their respective keys on their devices. The security and integrity of public key encryption depend on each private key being securely controlled by its owner, ensuring that only the intended recipient can decrypt messages and authenticate actions.

This exclusive control made possible by the design pattern of public key encryption maintains confidentiality and trust in digital communications, but also conflates each user’s digital devices with their real-world selves, creating a conceptual blind spot that, if not accounted for, results in real-world consequences. The most obvious consequence is the

[278] European Commission, European Digital Identity Wallets – Person Identification Data and Electronic Attestations of Attributes, last modified 3 June 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14340-European-Digital-Identity-Wallets-person-identification-data-and-electronic-attestations-of-attributes_en.

[279] European Commission, European Digital Identity Wallets – Protocols and Interfaces to Be Supported, last modified 3 June 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14339-European-Digital-Identity-Wallets-protocols-and-interfaces-to-be-supported_en.

[280] European Commission, ‘Implementing Regulation on European Digital Identity Wallets – Protocols and Interfaces to Be Supported’, 2024, https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-european-digital-identity-wallets.

[281] Rolf Oppliger, *Cryptography 101: From Theory to Practice*, Artech House, 2021.

overarching issue of social engineering attacks that is covered in this report. In the context of this finding, the conflation of human and device effects individual autonomy in unexpected ways, where the inability to disentangle from the exchange of data between our theoretical Alice and Bob results in autonomy loss in the real world. In interviews, research participants recounted several examples of overly-rigid implementations of secure digital identity resulted in loss of individual control, often with profound social consequences. One participant, who described herself as a professional technologist, described how the decisions by Apple Accounts designers directly contributed to her personal disempowerment and reinforcement of patriarchal hierarchies during and after her divorce from her husband:

> *"I am in an Apple Account family plan that is controlled by my ex-husband. There is no obvious way to separate our accounts, except for an ominous 'LEAVE FAMILY' button with UX that makes it seem more like a destructive button.*
>
> *We share custody of our two school aged children. If I leave this Apple family, I risk becoming the un-fun parent, where my children are frustrated when they stay and cannot access the entertainment in their own linked Apple Accounts. I want my kids to have the convenience of, for example, being able to rent a Marvel film at their Dad's house, and watch it at my house. That way, both households are equal, and my kids can focus on being kids. So, I have to keep this Apple Account.*
>
> *The other day, my ex-husband received a push notification that I had paid for a Tinder subscription, because his account is the 'admin' of our Apple family. We have been separated for some time now, I have a really amicable relationship with my ex and no personal concerns with him. But, still, he has no right to information about my sex life. As a professional working in technology, this entire experience has highlighted for me the ways in which financial control, stalking and domestic violence are not just enabled, but promoted through these immutable accounts."*
>
> Research participant
> Professional technologist

The implications of this coercive rigidity resonate broadly. Support networks for domestic violence survivors routinely navigate similar technological entrapments, and decoupling digital identities represents a common challenge experienced by support workers and activists working to help women leave violent relationships.[282] In Apple families, accounts

[282] Bridget Harris and Delanie Woodlock, 'Digital Coercive Control and Spatiality: Rural, Regional, and Remote

designated as 'Parents' are entrusted with financial decision-making and the management of personal data of all related accounts, including location data, device photos and videos, messages, and, potentially, detailed medical information.[283] Assigning such responsibility to a user is only really possible by relying on cryptographically secure digital identity model, driven by the philosophy of user-managed data sovereignty and personal computing.

According to Eurostat, in 2019 the European Union recorded a divorce rate of 1.8 per 1,000 persons, with an estimated 0.8 million divorces.[284] In the United States, the CDC's National Vital Statistics System reports declining divorce rates, with recent estimates indicating approximately 746,971 divorces annually.[285] When combined with the widespread efforts of domestic violence support systems to decouple victims from perpetrator, this anecdote demonstrates that the designers of Apple Account conceived and built a digital identity that, despite the company's marketing, fails to consider users as living beings beyond the keys within their devices. This is far from an edge case. Instead, such designs are a highly regressive view of human relationships, justified in part by the strict requirements of cryptography.

This is, of course, not unique to Apple. Similar family plans are available with every major tech platform, healthcare providers, grocery store chains, financial institutions and other every-day providers. In the case of relationship breakdown, the cryptographically secure digital identity enforces relations that result in significant loss of control and autonomy for a separating spouse, with potentially devastating consequences.

Beyond the conflation of user and device, the cryptographic primitives that enable secure digital identity have a second socio-technical limitation. By design, public key encryption relies on confidence in the association between public keys and the identities of the parties involved. Any uncertainty regarding key ownership can compromise security, as the effectiveness of the encryption depends on Alice and Bob using the correct public keys and safeguarding their private keys. Ensuring that public keys are correctly linked to their owners is essential for preventing security breaches like man-in-the-middle attacks or

Women's Experience'. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn, and Nicola Henry, 461-79, Emerald Publishing Limited, 2021, https://doi.org/10.1108/978-1-83982-848-520211030.

[283] Apple, 'Share Your Health Data in the Health App on iPhone', Apple Support, Accessed 12 June 2025, https://support.apple.com/en-gb/108323.

[284] Eurostat, 'Marriage and Divorce Statistics', *Eurostat Statistics Explained,* Last updated March 2024. Accessed 1 July 2025, https://ec.europa.eu/eurostat/statistics-explained/index.php/Marriage_and_divorce_statistics.

[285] Centers for Disease Control and Prevention, 'FastStats - Marriage and Divorce', *National Center for Health Statistics*, Last reviewed 14 February 2024, Accessed 1 July 2025, https://www.cdc.gov/nchs/fastats/marriage-divorce.htm.

attempts to subvert secure communication through methods such as backdoors, where unauthorised access points are inserted into the secure system for third-party access.

The fundamental assumptions underlying cryptographic identity systems, particularly the "one user, one device" paradigm, are directly challenged by Jennifer Harris's extensive research into technology access among homeless populations. Harris, a faculty member at the University of Bristol's School for Policy Studies, has documented how homeless people navigate digital systems. These institutionally mediated patterns, including supervised terminals, staff-gated Wi-Fi, time-boxed access, directly clash with secure-identity designs that assume exclusive device custody and uninterrupted user control, a set of observaions that, applied to our own observations, fundamentally contradict the exclusive control model that cryptographic security requires.

Harris's research reveals that device access is frequently institutionally mediated: supervised computer rooms, filtered access, limited hours, and staff-gated Wi-Fi are common; material constraints and rules shape what 'using technology' even means in practice. In 2024 study of social support organisations, Harris found that "*people with lived experiences of homelessness must increasingly negotiate digital technology to access resources related to housing, welfare benefits, employment, and support*" through shared access points and communal devices. Harris' observations directly undermine the work of cryptographers whose systems bind identity verification to individual device ownership; These systems cannot accommodate the collaborative technology practices that Harris documents as essential for survival.[286]

More critically, Harris's analysis of the digitisation of welfare benefits – systems that our own research demonstrates are increasingly moving toward cryptographic security models – reveals the exclusionary effects of rigid digital identity assumptions. Her research on the Her work on England's Universal Credit shows that the mandatory online application and management of claims, and the speed and scale of digitisation, proceed on homogeneous assumptions about users and risk marginalising the most vulnerable. The outcome is "*that many homeless people simply cannot meet the [the requirements set by digital identity and systems designers],*" and that, "*in making ICT use mandatory, homeless people will face significant barriers in trying to access welfare benefits online. These findings suggest that as technology comes to occupy an increasingly prominent role internationally within the provision of advice and other public and legal services, attention should be paid to the*

[286] Jennifer Harris, "Context Matters: Exploring the Mediated Nature of Digital Service Provision within Homelessness Organizations," *Mobile Media & Communication* 12, no. 2 (2024): 424-440, https://doi.org/10.1177/20501579231219842.

manner wherein varying social, material, and circumstantial trends within the lives of different groups of people, affect the nature, use, and impact of these systems."[287] These are barriers that cryptographic identity systems would only intensify.

In a separate study, Harris documents how technology access is mediated through institutional contexts that cryptographic individual sovereignty models cannot accommodate. In describing how vulnerable people access digital services via drop-in centers, night shelters, and support organisations, each with different rules, supervision levels, and technical capabilities, Harris finds that these mediated forms of access require a level of flexibility that cannot be accommodated by the systemic rigidity required to fulfil a cryptographic identity assumption that users independently control their authentication credentials. As Harris notes, "*the provision of technology within these settings was undoubtably affected by material constraints,*"[288] constraints that make individual cryptographic key management practically impossible.

Perhaps most significantly for cryptographic identity policy, Harris's research reveals that for individuals experiencing homelessness, technology needs vary dramatically based on crisis versus stability phases. During immediate crises, people require human-mediated identity verification and advocacy, support structures that cryptographic self-sovereignty models tend to eliminate. Harris found that, "*when people first become homeless, self-service digital channels of advice provision may not be suitable. The complexity of the participants' experiences and the intricacies of the process of navigating homelessness support systems, imply that human interactions and human communications are of vital importance in ensuring that homeless people receive timely.*"[289] Cryptographic identity systems that eliminate human override capabilities leave people unable to verify their identity precisely when they most need institutional support.

Harris's work is part of a growing body of research[290] [291] that demonstrates how digital identity systems – including cryptographically secure implementations – are "*built on core*

[287] Jennifer Harris, "The Digitization of Advice and Welfare Benefits Services: Re-imagining the Homeless User," *Housing Studies* 35, no. 1 (2020): 47-75, https://doi.org/10.1080/02673037.2019.1594709

[288] Jennifer Harris, "Context Matters: Exploring the Mediated Nature of Digital Service Provision within Homelessness Organizations," *Mobile Media & Communication* 12, no. 2 (2024): 424-440, https://doi.org/10.1177/20501579231219842.

[289] Jennifer Harris, "The Digitization of Advice and Welfare Benefits Services: Re-imagining the Homeless User," *Housing Studies* 35, no. 1 (2020): 47-75, https://doi.org/10.1080/02673037.2019.1594709.

[290] Justine Humphry, "Looking for Wi-Fi: youth homelessness and mobile connectivity in the city," *Information, Communication & Society* 24, no. 2, 2021, https://www.researchgate.net/publication/336106154_Looking_for_Wi-Fi_youth_homelessness_and_mobile_connectivity_in_the_city.

[291] Avgustis, Iuliia, Ibnelkaïd, Samira, and Iivari, Netta. 'Occupying Another's Digital Space: Privacy of Smartphone Users as a Situated Practice'. Computer Supported Cooperative Work (CSCW) 33, no. 1, 1 December 2024, https://doi.org/10.1007/s10606-024-09492-z.

assumptions underscoring current digital by default policies [that] warrant re-examining." In the case of homelessness, digital identity system form part of an apparatus that has a direct *inverse* impact on the efficiency and effectiveness of social support systems – contradicting the central claim made by proponents of digital identity. This is because such systems simply "*do not resonate with the lived reality of many homeless people.*"[292] This field, populated by studies from across the world and cultural contexts, together document how shared device usage, organisational mediation, crisis-driven needs, and collaborative survival strategies are actively disrupted by the 'one-user-one-device' paradigm.

Recent research by Sterre Den Breeijen and colleagues at the University of Groningen examined the gaps between legal and technical reality in SSI implementations, finding significant disconnects when applied to financial guardianship contexts created by official court procedures.[293] Whether motivated by cultural or economic reasons, such as the custom of families sharing a single device,[294] hundreds of millions of people living in digitised societies fall outside of the 'one user, one device' design assumption frequently relied upon by secure digital identity. In failing to acknowledge this reality, the disruptions experienced by these individuals – access to support services, user verification for services, privacy design, or even the ability to participate in the workforce[295] – risk becoming entrenched as digital identity continues to monopolise legal and civic representation of individuals.

Whether motivated by cultural or economic reasons, hundreds of millions of people living in digitised societies fall outside of the 'one user, one device' design assumption frequently relied upon by secure digital identity.[296] In failing to acknowledge this reality, the disruptions experienced by these individuals, which includes access to support services to the verification of individuals, to the design of privacy within these contexts,[297] the clash

[292] Jennifer Harris, "The Digitization of Advice and Welfare Benefits Services: Re-imagining the Homeless User," *Housing Studies* 35, no. 1 (2020): 47-75, https://doi.org/10.1080/02673037.2019.1594709.

[293] Den Breeijen, Sterre, van Dijck, Gijs, Jonkers, Tobias, Joosten, Rieks, and Zimmermann, Katja. 'Self-Sovereign Identity and Guardianship in Practice'. *European Journal of Law and Technology* 13, no. 3 (30 December 2022). https://ejlt.org/index.php/ejlt/article/view/895.

[294] Akter, Mamtaj, Das, Anik, Khan, Andaleeb, Ahmed, Syed Ishtiaque, and Kumar, Neha. 'It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-Based Privacy and Security for Mobile Smartphones'. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–8. CHI EA '23. New York, NY, USA: Association for Computing Machinery, 2023. https://doi.org/10.1145/3544549.3585904.

[295] Avgustis, Iuliia, Ibnelkaïd, Samira, and Iivari, Netta. 'Occupying Another's Digital Space: Privacy of Smartphone Users as a Situated Practice'. Computer Supported Cooperative Work (CSCW) 33, no. 1 (1 December 2024): 731–69. https://doi.org/10.1007/s10606-024-09492-z.

[296] Mamtaj Akter et al., 'It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-Based Privacy and Security for Mobile Smartphones', in Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems, 2023, 1–7, doi:10.1145/3544549.3585904.

[297] Payal Arora, 'Decolonizing Privacy Studies', Television & New Media 20, no. 4 (2019): 366–78,

between the Western paradigm of device ownership against the material reality of the wider world risks becoming entrenched as digital identity continues to monopolise legal and civic representation of individuals.

In interviews, research participants offered similar examples of the obstacles created by secure digital identity implementations. One participant, an I.T. systems professional working in private healthcare, described the data ethics and consent dilemmas arising from healthcare workers taking control of a secure digital identity during life-threatening situations:

> *“I’ve participated for a long time with global organisations that advocate for self-sovereign identity. These groups argue for the user to be in absolute control of their data. They are aiming for a world where users completely control their identity, and can not be coerced into sharing data without user consent. These groups expect this kind of design to function within wider society.*
>
> *I’m coming from the healthcare community. My response is, self-sovereign identity sounds great! But what happens when you’re unconscious on a gurney in the emergency room? How do you control your identity then? With digital health records, it’s necessary to override the individual’s self-sovereign ownership to inform treatment. In healthcare, we call this the ‘break the glass,’ situation. It’s at the healthcare provider’s discretion but is usually invoked in cases of mental crisis, physical trauma, and so on. Emergency conditions.*
>
> *There has to be ways, specific to the healthcare industry, where you can have an escape policy that says, ‘look, under these crisis conditions, you can learn everything that you want about me, because all of that can be applied towards potentially saving my life at the moment.’ There are many policy and ethics implications for these decisions, and I can’t say we have perfect answers to them. But that’s the reality.”*

Research participant
Healthcare Tech Consultant

~

The discrepancy between the one-user-one-device paradigm required to maintain control over a secure or self-sovereign digital identity is at odds with the realities of smartphone use by millions of users. Whether facilitating power of attorney, administering life saving

doi:10.1177/1527476418806092.

medical intervention, or supporting someone in an unstable economic situation, common to all examples of this issues are ways in which the identity system is routed around. We believe these situations will accumulate pressure within multiple areas of society, including healthcare, welfare services, financial services, childcare, etc. At the same time, they unintentionally act as opportunistic arguments for the legalisation of cryptographic backdooring, justified by the barriers that secure digital identities create when third-party access is required to function effectively in real-world contexts.

While different in intent from initiatives like the European Union's ChatControl proposals,[298] and the more recent United Kingdom request of Apple to introduce an OS-level backdoor into end-to-end encryption for law enforcement purposes,[299] they are similar in implementation insofar as they necessitate methods to bypass strict cryptographic safeguards to allow necessary access by authorised parties.[300] This convergence highlights a fundamental tension between maintaining strong cryptographic security and addressing the practical needs of diverse user populations.

~

The addition of newer cryptography design patterns further entrenches these assumptions. Zero-knowledge proofs (ZKPs) build upon asymmetric key encryption by enabling one party to prove they possess certain information without actually revealing the information itself. In simple terms, ZKPs work like a sophisticated game of "guess who," where a player (the prover) demonstrates knowledge of a secret without explicitly stating it, and another player (the verifier) confirms this proof without learning the secret.[301]

This capability is particularly valuable in contexts like traditional financial systems, blockchain networks, and public health records, where identity providers can promise user self-sovereignty via the individual-led management of both the security and the data contained within their digital identity when interacting with service vendors.[302] For example, in financial transactions, a ZKP design may enable a user to prove they have

[298] Council of the European Union, 'Draft Council Resolution on Encryption - Security through Encryption and Security despite Encryption', 20 November 2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-INIT/en/pdf

[299] UK Parliament, 'Online Safety Act 2023, Section 121', legislation.gov.uk, 2023, https://www.legislation.gov.uk/ukpga/2023/50/section/121.

[300] Council of the European Union, 'Draft Council Resolution on Encryption - Security through Encryption and Security despite Encryption', 20 November 2020. https://data.consilium.europa.eu/doc/document/ST-13084-2020-INIT/en/pdf

[301] Justin Thaler, *Proofs, Arguments, and Zero-Knowledge*, 3rd ed., Foundations and Trends in Theoretical Computer Science [Now Publishers, 2023], https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf.

[302] Lu Zhou et al., "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges, and Opportunities," *Journal of Information Security and Applications* 80 [February 1, 2024]: 103678, https://doi.org/10.1016/j.jisa.2023.103678.

sufficient funds without disclosing their exact account balance or any other identifying data to a third party.[303] In public health records, ZKPs can permit patients to verify their eligibility for certain treatments or vaccinations without revealing personal medical histories.[304] By reinforcing the one-to-one relationship between a user and their key or device, ZKPs ensure that cryptographic operations are securely tied to individual users, enhancing confidentiality and integrity in sensitive digital interactions.

However, ZKPs do not nearly solve the issue of consent their proponents claim. Not only do they entrench even deeper the model of cryptographically secured, one-device-one-person, personal computing – which remains deeply inadequate for exposed and oppressed communities – they also, in the broader debate surrounding the nature of consent, miss the forest for the trees. As Chris Wiggins and Matthew L. Jones put it in their historical study of computing and datafication:

> *“Privacy [...] can be viewed as an example of informed consent–where privacy is understood as circumstances around a disclosure of a fact, rather than the fact itself.”*[305]

While this principle can be read narrowly as the ability to disclose possession of the specific value of an attribute, it can also be understood as encompassing the larger socio-political implications of the necessity of such a disclosure. The power structures necessary for such requests are not questioned by this technical trick; they are merely skirted around. The democratisation of digital identity backed by the putative protections of ZKP could very well undermine decades-long efforts by activists warning against the dangers of relying on digital devices during arrests and identity checks. ZKPs, in fact, obscure the true power dynamics at play and inadvertently legitimise requests for sensitive data disclosures by authorities. In practice, they may amplify scenarios in which law enforcement officers demand direct access to personal devices under the pretext of verifying cryptographic proofs.

Activists have repeatedly stressed the risks associated with digital identity verification through smartphones:

> *“No matter what, teaching people they can add their IDs to their phones means some people will inevitably leave the house without physical ID, and that means creating the*

[303] Nihal R. Gowravaram, ‘Zero Knowledge Proofs and Applications to Financial Regulation’, *Harvard University*, 2018. http://nrs.harvard.edu/urn-3:HUL.InstRepos:38811528.

[304] John Reynolds, “Making a More Secure, Accessible Medical System with Zero-Knowledge,” *Aleo*, December 4, 2023, https://www.aleo.org/post/making-more-secure-accessible-medical-system-zero-knowledge/.

[305] Chris Wiggins and Matthew L. Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. W. W. Norton & Company, 2023.

> *opportunity for cops to demand phones – which you should never, ever do. Technical details of your digital ID aside, handing your phone to a police officer grants law enforcement a lot of power over some of your most intimate personal data. [...]*
>
> *"If police do have a warrant to search your phone, numerous courts have said they can require you to provide biometric login access via your face or finger [...]. The Fifth Amendment typically protects giving up passcodes as a form of self-incrimination, but logging in with biometrics often isn't considered protected "testimonial" evidence."*[306]

Wiggins and Jones directly address the discretionary power structures involved in the deployment of technological solutions such as AI, but their critique applies equally to cryptographic identity systems and identification processes:

> *"The aspiration to apply technical fix to problems in AI presumes that the use of AI is there to be improved, rather than pushed back or even resisted entirely. Lawyer and technology scholar Frank Pasquale identifies the movement to question even the building of systems as a "second wave" of algorithmic accountability: "While the first wave of algorithmic accountability focuses on improving existing systems, a second wave of research has asked whether the should be used at all – and, if so, who gets to govern them."*[307]

Thus, a similar critical lens should be applied to ZKPs and cryptographic identity systems more broadly: questioning not just their technical robustness, but also their fundamental societal and ethical appropriateness.

Further complicating the landscape is the fact that public-private key designs, including ZKPs, are fundamentally at odds with situations involving legal guardianship, power of attorney, and state oversight. All are contexts where individual digital autonomy must be legally overridden or transferred.[308] [309] Consider scenarios involving children of divorced

[306] Gaby Del Valle, 'Don't Ever Hand Your Phone to the Cops,' *The Verge*, 24 September 2024, https://www.theverge.com/2024/9/24/24252235/police-unlock-phone-password-face-id-apple-wallet-id.

[307] Chris Wiggins and Matthew L. Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. W. W. Norton & Company, 2023.

[308] While the Sovrin Foundation's white paper on guardianship acknowledges the difficulty of reconciling self-sovereign identity architectures with real-world legal constructs like guardianship, power of attorney, and custodial authority, its proposed solutions remain conspicuously abstract. The document calls for "a mechanism for non-consensual guardianship" and "revocable authorisations," but largely evades the constitutional and ethical quagmire this introduces, particularly in jurisdictions with entrenched family law or protective services. It is as if the foundational contradictions between liberal individualist cryptographic design and lived legal interdependence are treated as implementation details rather than first-order design flaws; Sovrin Foundation Guardianship Task Force, 'On Guardianship in Self-Sovereign Identity V2,' *Sovrin Foundation*,, 2023. https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper.pdf.

[309] Paul Grassi, Michael Garcia, and James Fenton, 'Digital Identity Guidelines: Enrollment and Identity Proofing,' NIST Special Publication 800-63A. *National Institute of Standards and Technology*, 22 June 2017. https://doi.org/10.6028/NIST.SP.800-63a.

parents, individuals under guardianship, or those who require power of attorney. In these cases, cryptographic digital identities designed to be immutable and exclusively bound to a single individual's device or credentials either have to be completely revoked or removed, rendering them legally useless, or they must be deliberately compromised through cryptographic backdoors, allowing a third party full operational control. This necessity for override or backdoor access directly undermines the fundamental security guarantees cryptographic identities claim to offer, exposing individuals to significant legal and practical vulnerabilities and challenging the ethical coherence of cryptographic self-sovereignty.

Such a scenario is already in motion, evident through ongoing global governmental efforts to mandate backdoors into encryption systems, often citing national security or law enforcement needs as justification. Should these overt attempts fail, governments could potentially leverage custodianship and guardianship scenarios as alternative avenues to compel system designers and platform providers into creating backdoors under the guise of legal and ethical necessity. Ignoring this emerging risk could lead to a future where cryptographic identity is systematically compromised, severely undermining the very security and trust these technologies initially sought to guarantee.

~

Our research clearly demonstrates that digital identity systems relying heavily on cryptographic security carry significant structural flaws that remain untested when implemented at a societal scale. By prioritising technical robustness over practical human realities, such systems inadvertently marginalise vulnerable groups, obstruct necessary legal interventions, and risk widespread socio-political manipulation. The fundamental assumptions underlying cryptographic identity, such as singular device ownership and immutable credentials, fail to acknowledge the complexity of human relationships and social practices, thereby creating dangerous gaps in both practical and ethical applicability.

It is imperative that policymakers, technologists, and civil society stakeholders urgently reconsider and redesign these systems. Digital identity must evolve to genuinely reflect the nuanced, complex nature of human society, ensuring security without sacrificing accessibility, flexibility, or legal accountability. Failure to address these issues now will not only exacerbate inequalities but also pave the way for unprecedented vulnerabilities and exploitation within digital infrastructures globally. ✳

6. Financialisation of digital identity accelerates fraud and erodes user privacy

“While [the shorthand information age*] may sum up neatly some key characteristics of contemporary societies, it is […] the implication of new technologies within the current restructuring of capitalism that gives that age its unique dynamic. They permit a new level of networking, particularly of financial flows, and they also make possible the globalization of capitalism. But the same restructuring also demands greater attention to detail, as competition, and awareness of risk, grows […]. And in order more exactly to determine the nature and extent of risk, more and more precise knowledge is sought. To decide question of eligibility, or even of guilt, the risk profile becomes crucially important. And in order to work properly, for most purposes it must also be attached to an accurate identity.”*[310]

~

Key Points

- › Digital identity is increasingly treated as a financial asset that is collateralised, speculated upon, and made immutable by design, to protect its assigned value.
- › Financialisation demands stable, verifiable identities, eroding user autonomy and undermining privacy across sectors.
- › KYC regimes and behavioural biometrics embed surveillance logics into identity systems, fuelling discriminatory profiling and structural fraud.
- › Blockchain and DeFi replicate centralised control under the guise of decentralisation, reinforcing exclusion and market capture.
- › Regulatory arbitrage enables global exploitation of identity systems through jurisdictional fragmentation and weak oversight.
- › Immutability incentivises identity theft, intensifies harm, and locks users into rigid verification systems with no path to recovery.
- › Identity infrastructure now prioritises market logic over human fluidity, flattening individuals into speculative instruments.

The transformation of identity attributes into tradeable financial assets creates systemic vulnerabilities that accelerate fraud while enabling regulatory arbitrage across jurisdictions. As identity data becomes collateral for financial products and KYC verification becomes extractive, fragmented regulatory enforcement allows entities to jurisdiction-shop for weaker oversight, making identity theft both more lucrative and more difficult to prosecute.

Financialisation can be defined as the process in which financial instruments mediate economic exchange, whereby both the number of instruments’ types, their complexity, and

[310] Jane Caplan and John Torpey, eds., *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton, NJ: Princeton University Press, 2001), https://press.princeton.edu/books/paperback/9780691009124/documenting-individual-identity

their abstraction, but also the volume of transactions, and their share of GDP, increase. "Incarnated in debts, shares, and a diverse array of financial products whose weight in our economies has considerably increased," financialisation makes "claims over wealth that is yet to be produced. Its expansion implies a growing pre-emption of future production."[311]

As Caplan and Torpey suggest in the quote introducing this finding, these "claims over wealth yet to be produced" cannot "work properly" without "[being] attached to an accurate identity." Claims by whom, and wealth produced where? Which conditions of payment, and between how many actors? As financial products grow in complexity and abstraction, so does the network of parties embroiled in their contractual obligations. Indeed, the weaponisation of documentation and identification sits at ground zero of the subprime mortgage crisis of 2008, with the rabid use of NINJA (no income, no job, no assets) loans "where aggressive mortgage lenders and brokers did not want any trouble qualifying otherwise non-qualifying loans."[312] In response, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 required increased information on a borrower's ability to repay a loan, including credit scores and employment information.[313]

~

As posited in an earlier finding, digital identity, tied to a vast array of emergent technological innovations, is the field resulting from a *cosmotechnics*, whereby moral claims are enshrined through technical means.[314] Just as its paper equivalents across history, digital identity as a whole is not merely a set of disparate technological gadgets, but rather forms, through its cosmotechnics, the basis of a broader political economy.

Since the financial crisis of 2008, infrastructural and operational logics of governance have been geared towards resolving the contradictions arising from the chaos ushered by the era of high financialisation. The political turmoil unleashed by the economic crisis in turn saw a blooming of novel technical apparatuses such as retail trading apps, so-called ethical assets, cryptocurrency and NFTs, challenging the old guard of finance, all-the-while stabilising its principles and moral claims in the mainstream. Indeed, "one of the enduring ironies of the

[311] Cédric Durand, *Fictitious Capital: How Finance Is Appropriating Our Future*, trans. David Broder [London: Verso, 2017], https://www.versobooks.com/products/320-fictitious-capital.

[312] Randall Dodd and Paul Mills, "Outbreak: U.S. Subprime Contagion," *Finance & Development* 45, no. 2 [June 2008]: 50-51, International Monetary Fund, https://www.imf.org/external/pubs/ft/fandd/2008/06/dodd.htm.

[313] Richard Cordray, "Prepared Remarks of CFPB Director Richard Cordray at the Consumer Advisory Board Meeting," Consumer Financial Protection Bureau, 30 March 2017, https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-chamber-commerce-11th-annual-capital-markets-summit/.

[314] Yuk Hui, *The Question Concerning Technology in China: An Essay in Cosmotechnics* [Falmouth: Urbanomic, 2022], https://urbanomic.com/publication/the-question-concerning-technology-in-china/..

financial crisis of 2008 is that these events did little to challenge Neoliberal rationalities, with markets continuing to be viewed as a response to all manner of social problems.”[315]

In parallel, increased industrial and informational competition from geopolitical contenders, such as the Chinese party-integrated industrial policy, and the Indian Stack, saw the U.S. and the EU alike launch countermeasures to re-establish a semblance of control over their perceived loss of sovereignty (TikTok ban, EU eIDAS Stack). All around the globe, nation-states and their diffuse network of actors, institutions and corporations have seized “processes of commercialisation and privatization” powering “technoscientific capitalism as a commodification movement that orients science and technology toward a market destiny.”[316]

A perfect example of this trend we’ve etched so far, where financial paradigms, technoscientific industrial policies and the “the paradoxical interests of accurate identification”combine, can be seen in invasive biometrics schemes. According to Magnet, these “[rise] to prominence at a time when the state is determined to make citizens newly visible for the purpose of governance.”[317] As she presciently noted in her review of the US-Canada NEXUS border system: ‘Allowing travellers to scan their body and providing them with a receipt of the transaction produces new understandings of the “body as commodity.” Biometrics break bodies down into their component parts in ways that allow them to be marketed more easily in the transnational marketplace, whether as a security risk or potential customer.’[318]

This analysis is strengthened by our research participants’ testimonies. During interview, a number of participants are anticipating the commodification of the body through digital identity:

‘These characteristics are interesting. I’d like to find out more about the individual, and see what else they’d be willing to share. Then they come back to me for more granular consent, but maybe there’s a contract now – that could be a smart contract, it could be a real life contract – that says “I’ll give you this percentage of my data for clinical research as part of drug developments but you’re going to give me $500.” Or if you participate in some sort of token economy, I think just setting up that structure around

[315] Kean Birch and Fabian Muniesa, eds., *Assetization: Turning Things into Assets in Technoscientific Capitalism* (Cambridge, MA: MIT Press, 2020), https://mitpress.mit.edu/9780262539173/assetization/.

[316] Ibid.

[317] Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham, NC: Duke University Press, 2011), http://www.dukeupress.edu/when-biometrics-fail.

[318] Ibid.

incremental data sharing with consent that leads to monetization as a incentive to do so, has really yet to be explored.'

Research participant
Independent health IT consultant

Following Muniesa et al.,[319] this processing of the body into market-friendly morsels by way of monopolies over technoscientific processes expands beyond commodification to become assetisation, *'a consequence of an emerging "asset form" that has come to replace the commodity as the primary basis of contemporary capitalism. By asset, we mean something that can be owned or controlled, traded, and capitalized as a revenue stream, often involving the valuation of discounted future earnings in the present,'* based not on market speculation so much as capital investment.[320] Indeed focusing on the pure speculation over morsels of data hides the forest for the tree. The huge outlays of capital to acquire talents, infrastructure, software and hardware, if often misguided and wasteful, determine long-term domination over given techno-scientific assembling and associated potential windfalls.

Our interviews confirm a vision of the future where a portion of the economy, such as consumer credit and start-up early investment, is collaterised and/or funded on the securitisation of people's healthcare attributes held within digital identity schemes. This is especially true in the age of the drying up of liquidities, with the tightening up of financing mechanisms such as the repo market. Similar solutions have already been tested at small scale over the past decade, such as *"the emergence of a new, investment-based funding model, the social impact bond (SIB)":*

"Pioneered in the UK in 2010, a SIB is an investment contract in which private investors provide up-front funding for a preventative program. If the program is successful in meeting predefined performance targets, the government repays the investment and provides a return based on the cost savings realized from reduced future demand on public services."[321]

While these schemes have so far shown to be poor receptacles of future revenue streams, the financial and informational principle at the heart of these tools have shown to be enduring and flexible, capable of exerting continuing influences on the very fabric of the non-profit and welfare State political economy:

[319] Kean Birch and Fabian Muniesa, eds., *Assetization: Turning Things into Assets in Technoscientific Capitalism* [Cambridge, MA: MIT Press, 2020], https://mitpress.mit.edu/9780262539173/assetization/.

[320] Ibid.

[321] Ibid.

> *"Utilizing the tools and lessons gleaned from their SIB work, the emphasis is on re-engineering existing spending streams using data analysis to identify inefficiencies in services, and performance management to exhort providers to address these inefficiencies and improve outcomes.[...] In mandating this valuation work and building contracts around the resulting outcomes, it is government that is ultimately taking on the role of investor extracting a type of public rent from the non-profit sector."*[322]

Once such financial and informational principle is fully institutionalised and operationalised at scale, the potential for catastrophic failures of custody, privacy, and care are extreme. As the increased scrutiny over digital advertising is just now starting to reveal the magnitude of the socio-technical threats ushered in its wake,[323] and as digital payments themselves are becoming national security risks,[324] the consequences when it comes to the financialisation of ID attributes are not hard to predict. First, the real danger to finance research in complex and speculative technology such as AI through pre-emptive assetisation of the product of digital identity systems. As one participant suggested:

> *"I think that assetisation leads to more finances that are available for us to do the work that we need to do. Whether that is technical work, whether that's paying the power bill to run the generative AI, whether that's hiring more researchers, funding more research, whatever it is, I think the assets can provide the finances that we need."*

Research participant
Researcher in generative AI and cognitive security

Regulatory arbitrage emerges as a critical yet overlooked dimension of the financialisation of digital identity, exacerbating systemic vulnerabilities through the exploitation of jurisdictional fragmentation. Recent FATF grey-listing demonstrates this dynamic: in June 2025, the British Virgin Islands and Bolivia were added to jurisdictions subject to increased monitoring due to "strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing."[325] These regulatory gaps create arbitrage

[322] Kean Birch and Fabian Muniesa, eds., *Assetization: Turning Things into Assets in Technoscientific Capitalism* (Cambridge, MA: MIT Press, 2020), https://mitpress.mit.edu/9780262539173/assetization/.

[323] Byron Tau, *Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State* (New York: Crown, 2024), https://www.penguinrandomhouse.com/books/706321/means-of-control-by-byron-tau/.

[324] Miranda Bryant, "Back to Cash: Life without Money in Your Pocket Is Not the Utopia Sweden Hoped," *The Guardian*, 16 March 2025 https://www.theguardian.com/technology/2025/mar/16/sweden-cash-digital-payments-electronic-banking-security.

[325] Financial Action Task Force (FATF), "Jurisdictions under Increased Monitoring," 13 June 2025, https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-june-2025.html.

opportunities where entities can jurisdiction-shop for weaker identity verification oversight.

These regulatory disparities fuel a global race-to-the-bottom, where jurisdictions seeking to attract foreign investment or competitive advantage intentionally relax oversight, allowing corporate entities to engage in riskier financial practices involving digital identities. The resultant arbitrage not only undermines individual privacy protections but also systematically weakens the capacity of states and local regulatory bodies to enforce consistent standards. Rather than strengthening identity accuracy and security, regulatory arbitrage encourages actors to bypass rigorous authentication, verification, and compliance protocols, further compounding financial risks and enabling fraudulent or exploitative financial practices on a global scale.

Moreover, regulatory arbitrage through jurisdictional fragmentation diminishes the efficacy of reactive legislative measures. As policymakers in jurisdictions such as the EU or the U.S. respond to abuses or systemic breaches by tightening regulations – such as GDPR enhancements, anti-money laundering requirements, or stricter Know Your Customer (KYC) rules – financial entities swiftly relocate sensitive identity-based financial operations elsewhere, where enforcement is weaker[326] through regulatory arbitrage[327] due to complex compliance burdens.[328] This mobility effectively neutralises protective regulations, perpetuating a cycle where remedial regulatory actions constantly lag behind shifting financial practices.[329] As a consequence, the global digital identity landscape becomes characterised by uneven enforcement, regulatory inefficiencies, and a perpetual state of systemic vulnerability.[330]

Finally, regulatory arbitrage further intensifies geopolitical tensions, transforming digital identity into yet another contested arena of influence. National governments leverage fragmented regulatory environments to reinforce political or economic objectives,

[326] Shuchishrabha Bhattacharjee and AM Akshaya, "Regulatory Arbitrage in Financial Markets: Causes, Consequences and Solutions," *Indian Journal of Integrated Research in Law*, September 2024, https://ijirl.com/wp-content/uploads/2024/11/REGULATORY-ARBITRAGE-IN-FINANCIAL-MARKET-CAUSES-CONSEQUENCES-AND-SOLUTIONS.pdf.

[327] Wolf-Georg Ringe, "Regulatory Competition in Global Financial Markets – The Case for a Special Resolution Regime," *European Business Organization Law Review* 17, no. 2 (2016): 283–310, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2659617.

[328] Danièle Nouy, "Too Complex to Function? Why We Need Simpler Rules for Financial Institutions," speech at the European Central Bank, 15 September 2017, arguing that regulatory complexity results from fragmented national rules and calling for harmonisation rather than deregulation, https://www.bankingsupervision.europa.eu/press/speeches/date/2017/html/ssm.sp170915.en.html.

[329] Tobias Adrian, Fabio Natalucci, and Mahvash S. Qureshi, "Fintech's Rapid Growth Calls for Stronger Policies," *IMF Blog*, International Monetary Fund, 13 April 2022, https://www.imf.org/en/Blogs/Articles/2022/04/13/blog041322-sm2022-gfsr-ch3.

[330] Financial Action Task Force, "High-Risk and Other Monitored Jurisdictions," 23 February 2024, https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

deploying identity systems both offensively to exploit rival states' regulatory weaknesses, and defensively by insulating their domestic systems from external accountability or intervention. The increasing intersection of state interests, corporate manoeuvring, and fragmented regulation creates profound vulnerabilities not only in financial markets but across diplomatic and political domains, making any single point of regulatory failure a potential trigger for broader economic or geopolitical instability.

Another critical intersection emerges within the financialisation of digital identity: the expanding regimes of Know Your Customer (KYC). Surveillance capitalism, whereby monetisation derives explicitly from granular consumer tracking,[331] has now intertwined deeply with the principles of financial identity verification. Major platforms and financial entities leverage identity systems not simply to authenticate users, but to profile and monetise behavioural patterns for profit.[332] KYC thus becomes not just a compliance mechanism, but a new form of value extraction – identity verification itself transforms into a commodity and a resource.[333] This commodification profoundly intensifies surveillance incentives, extending far beyond financial risk assessment to behavioural analysis and market prediction, thereby undermining user privacy under the pretext of enhancing accuracy or reducing fraud.

A striking manifestation of KYC's commodification is seen through the proliferation of behavioural biometrics, which claims to detect fraud or validate identity based on highly specific personal traits such as typing rhythm, mouse movements, and user interface interactions.[334] Embedded within KYC protocols, these behavioural markers are often presented as neutral or scientific measures of authenticity.[335] [336] [337] Yet, they encode unsubstantiated assumptions about human consistency, emotional states, and intentions, embedding biases and pseudoscientific interpretations into supposedly objective identity

[331] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019), https://profilebooks.com/work/the-age-of-surveillance-capitalism/.

[332] Julian Hope Wallace, "Surveillance Capitalism, the Commodification of Personal Behavioural Data, and How It Factors into Our Response" (MA thesis, University of Arizona, 2022), https://repository.arizona.edu/bitstream/handle/10150/665885/azu_etd_hr_2022_0146_sip1_m.pdf.

[333] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019), https://profilebooks.com/work/the-age-of-surveillance-capitalism/.

[334] Antony Seabra de Medeiros, Luiz Afonso Glatzl Junior, and Sergio Lifschitz, "Surveillance Capitalism Revealed: Tracing the Hidden World of Web Data Collection," arXiv preprint, https://arxiv.org/abs/2412.17944.

[335] Satish Lalchand, Jill Gregorie, and Val Srinivas, "Using Biometrics to Fight Back against Rising Synthetic Identity Fraud," *Deloitte Risk & Financial Advisory*, 27 July 2023, https://www.deloitte.com/us/en/insights/industry/financial-services/financial-institutions-synthetic-identity-fraud.html?id=us:2el:3dp:wsjspon:awa:WSJRCJ:2023:WSJFY24

[336] Chris Burt, "Biometrics Back Developing Shifts in KYC around the World," *Biometric Update*, 14 December 2024, https://www.biometricupdate.com/202412/biometrics-back-developing-shifts-in-kyc-around-the-world.

[337] Vineela Komandla, "Transforming Customer Onboarding: Efficient Digital Account Opening and KYC Compliance Strategies," SSRN Working Paper, 3 March 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4983076.

checks.[338] The result is a deeply flawed system in which KYC no longer acts merely as a fraud-prevention measure but instead contributes to algorithmically reinforced discrimination and social sorting. This implementation of behavioural biometrics within financial identity systems creates layers of exploitable surveillance, fostering invasive data collection while simultaneously failing to genuinely mitigate systemic fraud risks.[339]

Similarly, the ideological promises of decentralised finance (DeFi)[340] and blockchain-based identity systems provide yet another critical example of KYC becoming both economic and ideological value. Advocates claim these decentralised solutions democratise financial access, enabling trustless identity verification outside conventional institutional constraints. Yet, in practice, KYC protocols persistently re-emerge in supposedly decentralised contexts, infused directly into blockchain governance frameworks or encoded through compulsory token economies. DeFi platforms thus paradoxically recreate centralised surveillance patterns within decentralised architectures, forcing users to submit to ever-more extensive identity proofs as conditions for participation.[341] Consequently, rather than empowering marginalised users or reducing barriers to financial access, blockchain-based KYC protocols amplify traditional inequities.[342] They introduce novel forms of exclusion, wherein the refusal or inability to participate in detailed, invasive KYC procedures denies users the supposed benefits of decentralisation, exposing them instead to intensified market and surveillance logics.[343]

On a deeper level, however "decentralised" some of these solutions have prided themselves to be over the past two decades, they remain tied to rigid representations, probabilistic determinism and speculative design.[344] [345] Assetisation, blockchain and AI computations,

[338] Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, National Institute of Standards and Technology Special Publication 1270, (15 March 2022), https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence.

[339] Lauren Hendrickson, 'Privacy Concerns With Biometric Data Collection', *Identity*, 20 October 2024, https://www.identity.com/privacy-concerns-with-biometric-data-collection/.

[340] Decentralized Finance (DeFi) refers to a financial ecosystem that operates without central intermediaries, utilizing blockchain technology and smart contracts to facilitate peer-to-peer transactions. This system enables individuals and entities to engage directly in financial activities such as lending, borrowing, trading, and earning interest, bypassing traditional financial institutions. The core objective of DeFi is to democratize access to financial services, making them more accessible, transparent, and resistant to censorship; Raphael Auer et al., "The Technology of Decentralized Finance (DeFi)," *Bank for International Settlements*, 17 January 2023, https://www.bis.org/publ/work1066.htm.

[341] Meng Hou Sak, "KYC/AML Technologies in Decentralized Finance (DeFi)," Leonard N. Stern School of Business, Glucksman Institute (2024), https://www.stern.nyu.edu/sites/default/files/2024-07/Glucksman_Sak_2024.pdf

[342] Lynnise Phillips Pantin, "Financial Inclusion, Cryptocurrency, and Afrofuturism," *Northwestern University Law Review* 118, no. 3 (2023) https://scholarlycommons.law.northwestern.edu/nulr/vol118/iss3/5/.

[343] 'KYC in DeFi: Striking the Balance Between Compliance and Decentralization', *KYC Chain*, 14 February 2023, https://kyc-chain.com/?insight=kyc-in-defi-striking-the-balance-between-compliance-and-decentralization.

[344] Chris Wiggins and Matthew L. Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. W. W. Norton & Company, 2023.

[345] Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham, NC: Duke University Press, 2011), http://www.dukeupress.edu/when-biometrics-fail.

through the huge outlays of capital they imply, also drive monopoly, and therefore centralisation. As Silvia Masiero argues: *"The point holds for digital identity systems that present as decentralised: as shown in Cheesman (2022), such systems consist of technologies that, beyond the promotion of "self-sovereign identity", effectively crystallise the existing logics of control on beneficiary populations."*[346]

Indeed, decentralisation has frequently been promoted as an inherently liberatory architecture, implying diffuse power and increased autonomy for individuals.[347] [348] [349] Yet, in practice, the technological infrastructures underlying decentralised systems often conceal deeply centralising forces. Decentralisation, as commonly understood in digital identity and financial contexts, typically refers merely to the technical distribution of records or computational processes rather than meaningful political or economic decentralisation.[350] These protocols frequently require centralised oversight or gatekeeping mechanisms, such as token allocations, protocol governance committees, or consensus mechanisms dominated by a handful of large stakeholders.[351] Rather reproducing, and in some cases intensifying, the very power imbalances they claim to challenge.[352]

Moreover, decentralised identity systems rely fundamentally on representations of identity as stable, singular, and verifiable across contexts.[353] This rigid representational logic is inherently reductionist, systematically excluding fluid or marginalised identities unable or unwilling to align with rigid verification standards. Such systems, despite their technical distribution, are nonetheless rooted in probabilistic determinism, where identities and behaviours are algorithmically predicted, verified, and judged by probabilistic models.[354] The speculative designs of these systems not only diminish personal agency, but also

[346] Silvia Masiero, "Digital Identity as Platform-Mediated Surveillance," *Big Data & Society* 10, no. 1 (2023), https://doi.org/10.1177/20539517221135176.

[347] Danielle C. Robinson et al., 'The Dat Project, an Open and Decentralized Research Data Tool', *Scientific Data* 5, no. 1 (23 October 2018): 180221, https://www.nature.com/articles/sdata2018221,

[348] Geoff Goodell and Tomaso Aste, 'A Decentralized Digital Identity Architecture', *Frontiers in Blockchain* 2 (5 November 2019), https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2019.00017/full.

[349] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 31 October 2008, https://bitcoin.org/bitcoin.pdf.

[350] Zizheng Fonghu and Tsz Hon Yuen, 'A Critique on Decentralized Finance from a Social, Political, and Economic Perspective', *Blockchain* 1, no. 1 (31 March 2023): 1–2, https://www.elspub.com/papers/j/1597124912186978304.html.

[351] Lin William Cong et al., 'Centralized Governance in Decentralized Organizations', *SSRN* Scholarly Paper (Rochester, NY: Social Science Research Network, 1 March 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5168660.

[352] Ashish Rajendra Sai et al., 'Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review,' arXiv, 26 September 2020, https://arxiv.org/abs/2009.12542.

[353] Marina Meira, Digital Identity Systems and the Exclusion of Marginalised Communities: Proposing Paths to Mitigate Fundamental Rights Violations (presentation, The Alan Turing Institute, London, 4 November 2022), *YouTube*, posted by The Alan Turing Institute, 4 November 2022, https://www.youtube.com/watch?v=tR4YQonv_I8.

[354] Michael Kubach et al., 'Self-Sovereign and Decentralized Identity as the Future of Identity Management?', *Open Identity Summit*, 2020, https://dl.gi.de/bitstreams/aaa640a1-f8dd-4514-ad72-b809932072cc/download.

obscure the subjective and political assumptions embedded within them, concealing centralised forms of decision-making behind the veneer of neutrality or impartiality.[355]

Ultimately, decentralisation in digital identity and financialisation narratives functions more as a rhetorical device rather than a genuine structural shift. As large financial actors invest heavily in blockchain and related decentralised infrastructures, their economic dominance translates directly into disproportionate influence over these seemingly neutral technologies. Thus, rather than dismantling centralised authority, decentralisation can paradoxically reinforce monopolistic tendencies, consolidating economic power within select entities capable of mobilising sufficient resources to govern the protocols themselves. This dynamic demonstrates that decentralisation, absent genuine political or economic restructuring, is at best incomplete and at worst actively deceptive, masking concentrated control under the guise of distributed empowerment.

~

An ad-hoc *proto-market* of solutions thus accelerates fraud: multiplying private identity systems, wallets, and identity managers embedded within rapidly proliferating marketplaces. With each new service introduced, digital identity not only controls access but itself becomes a vulnerable point of systemic failure. Underpinning these digital identity schemes is the financial industry's pervasive fixation on stable, immutable identity. This fixation fundamentally conflicts with human reality: lives are fluid, identities evolve, and personal circumstances shift continuously, whether by choice or necessity. Yet, the architecture of financialised identity assumes precisely the opposite: a stable, singular self, readily verifiable and invariant across contexts.

This insistence upon immutability masks a critical misalignment: identity design is no longer simply about establishing trust or minimising risk, but inherently generating economic value.[356] The market incentivises the design and proliferation of systems that prioritise immutability, precisely because immutability itself is financially valuable and trusted. As a consequence, verifiable identities represent a form of collateral in their own right, anchoring assetisation and securitisation of data streams. Rather than identity serving primarily as a means of authentication, authentication becomes commodified.[357]

[355] Molly White, 'Is "Acceptably Non-Dystopian" Self-Sovereign Identity Even Possible?', *Molly White blog*, 10 June 2022, https://blog.mollywhite.net/is-acceptably-non-dystopian-self-sovereign-identity-even-possible/.

[356] Anu Madgavkar, Olivia White, James Manyika, Jacques Bughin, Michael Chui, and Jonathan Woetzel, 'Digital identity: A key to inclusive growth.' *McKinsey Global Institute*, 17 April 2019, https://www.mckinsey.com/industries/public-sector/our-insights/digital-identification-a-key-to-inclusive-growth.

[357] Robles-Carrillo, Margarita, 'Digital identity: an approach to its nature, concept, and functionalities.' *International Journal of Law and Information Technology* 32, no. 3 (Autumn 2024): 255-287

The dynamic is self-reinforcing, generating designs whose fundamental assumptions remain largely unquestioned precisely because their profitability seems self-evident. The underlying logic, unchallenged due to financial incentives, distorts identity away from personal autonomy and towards rigidified economic constructs.[358]

Such unquestioned designs find stark expression in the rhetoric and architecture differences between national identity schemes. Estonia's Digital ID, originally developed explicitly as a civic technology, emphasises interoperability, state accountability, and access as citizen rights.[359] Contrast this with the EU Digital Identity Wallet, whose framing is deeply financialised, emphasising convenience, marketplace integration, and cross-border transactions, explicitly invoking the term "wallet" to anchor its identity scheme in commercial logic.[360] This linguistic and conceptual shift – from citizen-centred civic rights to consumer-centred financial management – reveals the ideological embedding of immutability as a commercial imperative. The comparison underscores how identity fluidity is actively eroded, replaced instead by financialised conceptions of personhood as stable economic agents.

The emphasis on immutability thus paradoxically amplifies the financial risks it ostensibly seeks to mitigate. If an identity's economic value hinges upon its permanence, then the incentive to steal, manipulate, or fabricate such immutable identities grows dramatically. The identity becomes extraordinarily valuable as a financial asset; Consequently, identity theft transitions from being merely opportunistic fraud to a strategic investment. Once enforced, immutability ensures stolen identities retain market value, thus intensifying the appeal of identity theft, rather than deterring it. The consequences are profound: permanent and highly valuable identities cannot easily be revoked, corrected, or contested, leaving individuals permanently exposed to harm.

Blockchain and decentralised finance (DeFi) offer instructive but incomplete examples of this contradiction. State-driven digital identity schemes and newer financial protocols such as credit-scoring systems further illustrate the dangers of immutable financialised identity constructs. Once credit scores, state-benefit entitlements, or healthcare statuses become rigid and immutable, the consequences of identity theft or error become catastrophic. Each successful breach creates lasting, potentially irreversible damage to personal livelihoods.

https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaae019/7760180.

[358] Marianne Díaz Hernández, 'Why we need tailored identity systems for our digital world', *Access Now*, 11 September 2024, https://www.accessnow.org/digital-identity-systems/

[359] Shruti Trikanad, *Governing ID: Estonia's E-Identity Programme* (Bangalore: Centre for Internet & Society, Apr. 2020). https://digitalid.design/docs/CIS_DigitalID_EstoniaCaseStudy_2020.04.pdf.

[360] Alexander Reithoffer, "Understanding the European Digital Identity Wallet," *[ISC]^2 Insights*, 8 Apr. 2025. https://www.isc2.org/Insights/2025/04/Understanding-the-European-Digital-Identity-Wallet.

Moreover, attempts to mitigate fraud risks through increasingly rigorous, rigid verification paradoxically deepen systemic fragility. Identities that are by immutable by design are the most difficult to recover or rectify once compromised.

Ultimately, the financial industry's fixation on identity immutability, far from enhancing security or reliability, is driving the digital identity ecosystem towards catastrophic risk. The relentless pursuit of stable, commercially valuable identities suppresses the reality of human fluidity, creating conditions in which fraud is incentivised, identity theft is lucrative, and personal security becomes paradoxically contingent upon rigid, irreversible digital constructs. As digital identity continues to be financialised, the danger is clear: identities themselves risk becoming irrevocably monetised, compromised, and weaponised: an event horizon beyond which recovery may prove impossible.

~

The financialisation of digital identity has restructured the conditions of access, trust, or authentication, and in the process created a new political economy in which the identity itself becomes collateral, infrastructure, and speculative asset. Our research shows this transformation is not hypothetical nor confined to theory. Across our interviews, participants from diverse positions that included end users, technical vendors, institutional procurement leads and policy designers, consistently described the growing institutional unease with the permanence and rigidity demanded by KYC regimes. Their discomfort spans every tier of the digital identity stack: users struggle to correct or revoke identity attributes once attached to services; vendors are locked into brittle verification flows that fail to accommodate edge cases or shifts in circumstance; and identity providers face growing pressure to monetise verification itself as a form of value, while absorbing the liability of systemic fraud.

The tensions borne from the enmeshment of financialisation, identity markers as proof-of-personhood or KYC and data permanence are not edge cases. Rather, they are universal and endemic to the architecture of financialised identity systems. The promises of risk reduction, fraud prevention and user empowerment increasingly appear hollow when compared against the structural incentives shaping design: identity systems that cannot accommodate change; decentralised systems that obscure centralised control; and compliance regimes that become extractive by design. What we are witnessing is not simply a privacy crisis or a security failure, but the consolidation of a market logic where human identities must be frozen, flattened, and financialised to be deemed legible. What follows is both an acceleration of fraud and an institutional paralysis, The question is not whether these systems work, but who they are designed to work for. ✳

7. Proof-of-personhood mechanisms incentivise AI-powered social engineering vulnerabilities

Key Points

- Proof-of-personhood schemes can increase social engineering risk by financialising identity and amplifying attack incentives.
- These systems embed behavioural norms into infrastructure, punishing deviation and reinforcing conformity at scale.
- Identity becomes a commodified, transferable proof that can be exploited by adversaries, state actors, and corporate systems alike.
- Verification systems that conflate personhood with legitimacy are vulnerable to manipulation through coercion, context mimicry, and AI-powered spoofing.
- The assumption that identity can be securely proven erases the relational, contingent, and performative nature of how people are recognised and trusted.
- Once breached, identity systems do not fail gracefully. Instead, they cascade, weaponising trust as an exploit vector across institutions and infrastructures.

Since 2010, disinformation campaigns, bot networks, and sophisticated social engineering attacks have surged, fostering a hostile data society and a corresponding collapse of trust in digital systems.[361] This escalation is largely due to the unintended leakage inherent in the systems of over-datafication central to surveillance capitalism, where personal data is commodified and often mishandled.[362] Such scams frequently rely on the weaponisation of digital identity through social engineering, or on identifying potential targets through their online personas. To combat these threats, emerging digital identity models advocate for the use of *proof-of-personhood*: cryptographic techniques that verify a user's unique human identity without revealing sensitive personal information as a defence tactic to reliably identify humans within a network.[363] [364]

Our research indicates that while these methods introduce a potentially effective means to separate humans from automations in a digital system, proof-of-personhood also inadvertently increases the value of data used for digital identity verification as a second-order consequence. This amplification heightens the risk of such data being weaponised for social engineering attacks, often in ways that have yet to be seen in the digital security field. As a result, the deployment of proof-of-personhood models without corresponding efforts to limit over-datafication or over-financialisation creates

[361] Global Risks Report 2024 press release, *World Economic Forum*, 10 January 2024, https://www.weforum.org/publications/global-risks-report-2024/.

[362] European Data Protection Board, Security of Processing and Data Breach Notification: OSS Case Digest, January 2024, https://www.edpb.europa.eu/system/files/2024-01/one_stop_shop_case_digest_security_data_breach_en.pdf.

[363] Vitalik Buterin, "What Do I Think about Biometric Proof of Personhood?" blog post, 24 July 2023. https://vitalik.eth.limo/general/2023/07/24/biometric.html

[364] Sebastian Barros, "Proof of Humanity: A Multi-Layer Network Framework for Certifying Human-Originated Content in an AI-Dominated Internet," arXiv preprint, 2 April 2025. https://arxiv.org/abs/2504.03752.

powerful new financial incentives for adversaries, where an attacker can coerce individuals into misusing their proof-of-personhood in new ways and often without a clear understanding of the associated risks.

This dynamic is not incidental, but instead reflects the broader trend of financialisation of identity infrastructures, where proof-of-personhood becomes not both a trust mechanism and a market device. As identification systems are linked to financial products, tokenised credentials, and platform entitlements, the cost of identity loss increases, and so too does its value to coercive actors.[365] The effect is perverse: verification becomes leverage. Systems designed to empower individuals instead render them more extractable, especially in contexts of instability, precarity, or asymmetric dependency. As Zuboff observes in *The Age of Surveillance Capitalism*, the economic logic of data extraction thrives not merely on visibility, but on behavioural predictability and control.[366] Proof-of-personhood risks aligning perfectly with this logic, offering systems a more trustworthy substrate from which to generate compliance and profit, whether by choice or by force.

~

In early 2020, researcher Francis Tseng described the then-coming decade as one of ‘meta-scams.’ Tseng theorised that users would recognise the rising data-fuelled power wielded 2010s-era digital platforms – then euphemistically described as the *‘sharing economy’* –and meet their predatory practices via a series of ‘interventions [that] disrupt a scam by turning it against itself or by using another scam against it, flipping its original power gradient.”[367] In essence, users would leverage the data accessible to them within surveillance capitalism[368] to manipulate pricing algorithms or socially engineer platforms for their own benefit.

Five years on, Tseng’s prediction has only partially materialised. Instead of users subverting the system as a form of collective power, such efforts to manipulate systems have fragmented and individualised. As surveillance capitalism has accelerated unchallenged, it over-identifies and over-datifies entire populations, liberally leaking its own contents in the process. The result is a near-perfect storm of opportunity: Ease of access to personal

[365] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly and Bryan Ford, Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies [Lausanne: École Polytechnique Fédérale de Lausanne, 29 April 2017], https://berkeley-defi.github.io/assets/material/Proof%20of%20Person.pdf.

[366] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* [London: Profile Books, 2019], https://profilebooks.com/work/the-age-of-surveillance-capitalism/.

[367] Francis Tseng, “The Art of the Meta-Scam,” *Rhizome* blog, 1 April 2020, https://rhizome.org/editorial/2020/apr/01/the-art-of-the-meta-scam/.

[368] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* [London: Profile Books, 2019], https://profilebooks.com/work/the-age-of-surveillance-capitalism/.

data, ubiquitous internet connectivity, increasing reliance on social media platforms, and advancements in machine learning all combine to democratise the adversarial tools required for social engineering attacks. Social engineering attacks were already considered amongst the largest threats to cybersecurity by as early as 2009.[369] Yet, despite various software solutions and user awareness campaigns, adversaries continues to leverage digital identity to target individuals for a variety of objectives. The situation threaten to collapse public trust in digital systems and is clearly untenable.

To combat such adversaries, designers of digital identity propose new systems. One result is the concept of proof-of-personhood, a method for verifying human ownership of digital identities that relies heavily on extensive personal identity markers, including behavioural data and biometrics.[370] Often intertwined with the financialisation of digital identity through mechanisms like identity tokenisation in Web3,[371] data brokerage as anti-fraud measures,[372] and financial authorisation processes, proof-of-personhood has magnified the value of personal information in ways that remain poorly understood.

Tseng's anticipation of collective subversion through coordinated scams has, in practice, devolved into isolated acts of manipulation. This shift is not a mere byproduct of technological evolution but a consequence of deliberate system design. Proof-of-personhood mechanisms, while ostensibly enhancing security, have inadvertently fragmented collective resistance.[373] By enforcing unique, verifiable identities, these systems deter large-scale, coordinated actions, compelling individuals to operate alone. This isolation not only diminishes the potential impact of subversive efforts but also increases the vulnerability of individuals to detection and punishment.[374] The architecture of proof-of-personhood, therefore, serves to atomise dissent, reinforcing systemic control under the guise of safeguarding digital interactions.

[369] Marc Fossi et al., Symantec Internet Security Threat Report, Vol. XV: Trends for 2009 (Mountain View: Symantec, 5 April 2010), 23-24, https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/2009-Symantec-Internet-Security.pdf.

[370] InterLink Labs, "InterLink ID: Proof of Personhood," white-paper, 2024, https://whitepaper.interlinklabs.ai/proof-of-concept/interlink-id-proof-of-personhood.

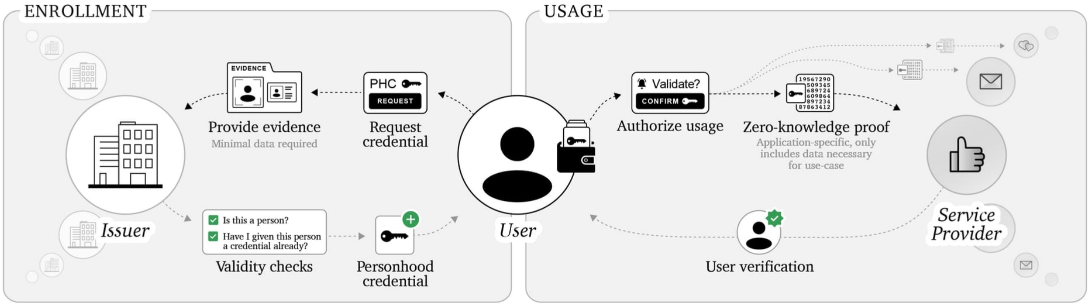
[371] Binance Academy, "What Are Soulbound Tokens (SBT)?" 17 August 2022, updated 11 November 2022, https://academy.binance.com/en/articles/what-are-soulbound-tokens-sbt.

[372] European Banking Authority, Opinion on the Elements of Strong Customer Authentication under PSD2 (London: EBA, 21 June 2019), https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf.

[373] Puja Ohlhaver, Mikhail Nikulin and Paula Berman, Compressed to 0: The Silent Strings of Proof of Personhood (working paper, last revised 11 April 2024), *SSRN*, https://ssrn.com/abstract=4749892.

[374] Divya Siddarth, Sergey Ivliev, Santiago Siri and Paula Berman, "Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols," Frontiers in Blockchain 3 (12 November 2020), https://www.frontiersin.org/articles/10.3389/fbloc.2020.590171/full.

Privacy-preserving enrollment and usage of personhood credentials (PHCs)



PRIVACY PROPERTIES

- Issuer carries out validity checks by processing minimal information while allowing for credential recovery and revocation
- Usage activity is inaccessible to issuer

- Service provider learns nothing about user beyond the fact that they hold a valid PHC
- Different service providers cannot link users because each proof is application-specific

This inflation in value does not occur in isolation. Proof-of-personhood mechanisms, especially those intertwined with financial infrastructures such as Web3 identity tokens, gradually convert identity into a financial instrument of exchange, speculation, and collateral.[375] [376] After transformation, personhood is no longer bound to the body, the voice, or even social relation. Instead, personhood becomes a unit of value within adversarial markets to be traded and abstracted until it exists more as proof-commodity than identity. The mechanisms mirror the broader logic of commodification, where social and relational markers are transformed into exchangeable assets. Amongst the most potent examples of the transformation and commodification of identity are Web3 proposals like Vitalik Buterin's Soulbound Tokens,[377] which flatten identity into quantifiable, tokenised permanence. Even the most optimistic designs based on decentralised identifiers, non-transferable credentials and Sybil-resistance schemes[378] rely on the same infrastructural logic: Identity is something to be financialised and securitised, not lived.[379] Such proofs, once extracted, circulate independently of the individual they once verified. They enable fraud, impersonation, or coercive transactions, where one's biometric attestation becomes a transferable burden. The more secure the proof, the more valuable its theft;[380] the more abstract the identity, the less recoverable the person.

[375] Decentralized Identity Foundation, "Balancing Online Trustworthiness and Anonymity with Personhood Credentials," *Decentralized Identity Foundation* [blog], 15 August 2024, https://blog.identity.foundation/balancing-online-trustworthiness-and-anonymity-with-personhood-credentials/.

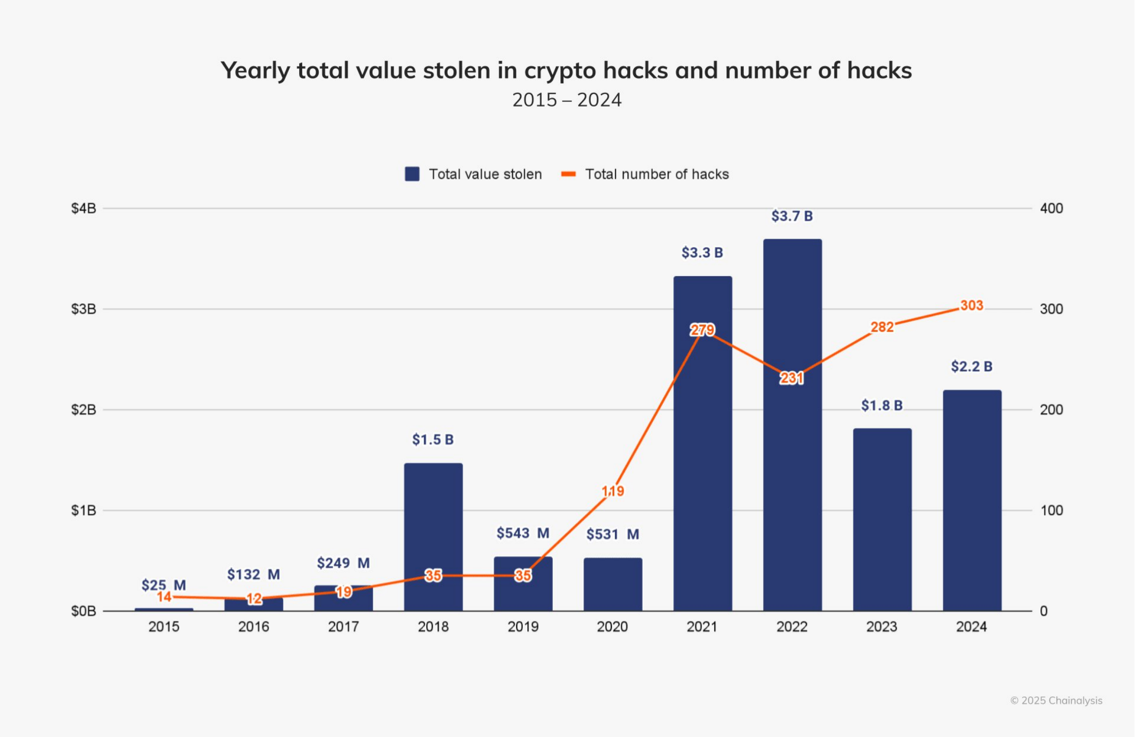
[376] McKinsey & Company, "What Is Tokenization?" McKinsey Explainers, 25 July 2024, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization.

[377] E. Glen Weyl, Puja Ohlhaver and Vitalik Buterin, "Decentralized Society: Finding Web3's Soul," Working paper, 10 May 2022, *SSRN*, https://ssrn.com/abstract=4105763.

[378] Paul Inglis, "Why Your Biometric Data Will Soon Be More Valuable than Money," *TechRadar*, 2 June 2025, https://www.techradar.com/pro/why-your-biometric-data-will-soon-be-more-valuable-than-money.

[379] World Bank, "Tokenization," in *Identification for Development Practitioner's Guide* [Washington, DC: World Bank, n.d.], https://id4d.worldbank.org/guide/tokenization.

[380] David Geer, "Cybercriminals Eye Biometrics," *Communications of the ACM* 65, no. 7 [23 June 2022], https://cacm.acm.org/news/cybercriminals-eye-biometrics/.



© 2025 Chainalysis

Figure: An overview of the economic cost and frequency of Web3 and cryptocurrency attacks. Social engineering attacks on digital identity is a frequent core role in a successful criminal theft operation.[381]

Yet even as these systems claim to validate identity neutrally and securely, and even as the wider context of social engineering demands the defences of proof-of-personhood, they operate on unexamined assumptions about behaviour and legitimacy. In order to determine both the baseline of personhood, and to identify unauthorised access, proof-of-personhood schemes must define what counts as "normal" behaviour in order to distinguish authentic users from bots or bad actors.[382] But this demand is always rendered through machine-readable data – and as a result, turns trust into a statistical expectation. The question of who gets to be verified quickly becomes a question of who conforms. In countries like China and Venezuela, where digital identification systems are used to monitor and discipline populations, behavioural scoring has already become central to political and social exclusion.[383] [384] [385] Individuals who deviate due to activism, poverty, neurodivergence, or for

[381] Chainalysis Team. "Chart: 'Total Value Stolen in Crypto Hacks and Number of Hacks, 2015-2024.'" In Elina Moskovchuk, "2024 Crypto Hacks Total $2.2 Billion in Losses," The Coinomist, December 24, 2024. https://coinomist.com/opinions/2024-crypto-hacks-total-dollar22-billion-in-losses/.

[382] Brendan Pelto, Mounika Vanamala, and Rushit Dave, "Your Identity Is Your Behaviour - Continuous User Authentication Based on Machine Learning and Touch Dynamics," arXiv preprint, 2023, https://arxiv.org/pdf/2305.09482.

[383] Xu, Xu, Genia Kostka, and Xun Cao, "Information Control and Public Support for China's Social Credit System." Journal of Politics 84, no. 4 (October 2022), https://www.journals.uchicago.edu/doi/10.1086/718358.

[384] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control." *Reuters*, 14 November 2018. https://www.reuters.com/investigates/special-report/venezuela-zte/.

[385] Charlie Campbell, "'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means

any other reason, are more likely to be flagged as anomalies[386] and excluded from services or legal protections.[387]

The problem is not limited to authoritarian contexts. As the Organisation for Ethical Source notes, *trust itself can be weaponised as a coercive tool:* “trust” becomes the currency that individuals must continuously perform, rather than a shared foundation of social relation.[388] Once baseline behaviours are encoded into infrastructure, deviation becomes synonymous with risk, even when that deviation is necessary, ethical, or simply different. The result is a constellation of systems that entrench desired behaviours by predicting and enforcing actions in ways that quietly erode autonomy. In the assumption that identity is stable and legible, proof-of-personhood risks foreclosing on the possibility that personhood might be messy, negotiated, or contested.

Digital identity systems, particularly those employing proof-of-personhood mechanisms, do more than verify identity. They actively shape and enforce behavioural norms. By defining and codifying what constitutes ‘normal’ or ‘acceptable’ behaviour, these systems move beyond passive observation to active intervention, creating predictive feedback loops that influence user actions. This phenomenon aligns with Judith Butler’s concept of performativity, where identity is not merely expressed but constructed through repeated actions within a regulatory framework.[389] In the context of digital identity, users may alter their behaviours to conform to the expectations embedded within these systems, leading to a homogenisation of actions and a suppression of individuality. For instance, social networking sites often encourage users to present themselves in particular ways, influencing identity formation and self-presentation.[390]

Moreover, these predictive systems can perpetuate existing biases. By relying on historical data to forecast and enforce norms, they may reinforce societal prejudices, leading to discriminatory outcomes. This raises critical questions about agency and autonomy in digital spaces, as individuals find themselves navigating environments where their

for the Rest of the World.” *Time*, 21 November 2019, https://time.com/5735411/china-surveillance-privacy-issues/.

[386] Paul Hebert, “AI Systems Show Alarming Bias Against Neurodivergent Communication Patterns,” *Algorithm Unmasked*, 14 May 2025, https://algorithmunmasked.com/2025/05/14/ai-systems-show-alarming-bias-neurodivergent-communication-patterns/.

[387] Burgess, Matt, Evaline Schot, and Gabriel Geiger. “This Algorithm Could Ruin Your Life,” *Wired*, 6 March 2023. https://www.wired.com/story/welfare-algorithms-discrimination/.

[388] Organisation for Ethical Source, “Ethical Source: Open Source, Evolved,” 2024, https://ethicalsource.dev/.

[389] Judith Butler, *Gender Trouble: Feminism and the Subversion of Identity* (London: Routledge, 1990).

[390] Rob Cover, “Performing and Undoing Identity Online: Social Networking, Identity Theories and the Incompatibility of Online Profiles and Friendship Regimes,” *Convergence: The International Journal of Research into New Media Technologies* 18, no. 2 (May 2012): 177–193, https://doi.org/10.1177/1354856511433684.

behaviours are not only monitored but also moulded by underlying algorithms.[391] The performative nature of digital identity thus becomes a double-edged sword, offering avenues for self-expression while simultaneously constraining that expression within predefined boundaries.[392]

These new methods of attack are already in use. Over the period of this research, hundreds of examples have already made the mainstream news cycle, thanks in no small part to the boom of biometric-secured devices paired with the widespread use of smartphone-housed credentials and financial products. The cryptocurrency and NFT craze and their physical wallets have made the criminal access to huge sums of money trivial; but the increased reliance on handheld devices to house anything from public transportation passes, credits and debit cards, retail-consumer stocks and official travel documents has turned millions of peoples' s smartphones into a social-engineering dream:

> *"People can be walking with millions of dollars in their pocket. A simple face scan, a fingerprint on the mobile phone, and there could be sat generational wealth."*[393]

For many research participants, the new horizon of threats, intensified by new adversarial strategies and accelerated by LLMs have become a new daily reality. Participants whose professional work tended towards private white hat consultancies or open source intelligence (OSINT) often shared their encounters with such attacks in the wild:

> *"I saw an APT (Advanced Persistent Threat) attacker targeting a CEO of a large defence contract company. They compromised the CEO's daughter, and lurked on her social media for a period of time. An opportunity presented itself to target the CEO when his daughter was vacationing in Mexico. The APT sent a phishing email to the CEO from her email containing pictures from her vacation that were loaded with malware. They leveraged the familial relationship with his daughter to infect his laptop. Being CEO, he had access to literally everything. He was completely pwned.*
>
> *The CEO was horrified that he had allowed this to happen. This was the company that he was a head of. Psychologically, I know it took an enormous toll on him. His company was a defence contractor, and the APT was after national security and defence information."*

[391] Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *The British Journal of Sociology* 51, no. 4 (December 2000): 605-622, https://doi.org/10.1080/00071310020015280.

[392] Solon Barocas, Moritz Hardt and Arvind Narayanan, *Fairness and Machine Learning: Limitations and Opportunities* (online pre-publication ed., 2022), https://fairmlbook.org/.

[393] Kira YT, "Why You Should Never Talk About Money Online," *YouTube*, 3 May 2024, https://www.youtube.com/watch?v=XSvbr6pDjvk.

Research participant
Cybersecurity consultant

While the information security discipline might classify such an event as a lapse in operational security,[394] what this anecdote really illustrates is the fragility of a system that centralises identity, access, and trust in a singular, verifiable personhood. The CEO was not compromised despite proof-of-personhood infrastructures, but *because of them*.

Through a pure information security lens, the design of digital identity, augmented by proof-of-personhood, carries a high risk of becoming a liability. As generative AI becomes more accurate at mimicking human language, behaviour, and biometrics, it further destabilises trust in identity systems that rely on fixed attributes and clean data pathways. Adversaries can now simulate plausible interactions at scale beyond phishing emails, analysing entire behavioural profiles,[395] voice and face information,[396] and other highly personal identity markers. Current identity systems have no meaningful defence against this class of attack[397] [398] – most defense systems are built on the shaky assumption that fraud detection is an arms race of features and heuristics rather than the fabrication of input data completely. But social engineering is not a technical glitch. Social engineering is, at its core, a structural failure of identity models that ignore coercion, mimicry, and cognitive overload. With the rise of generative AI capable of faking such data, social engineering finally becomes mechanised and automated.[399] [400]

But beyond the immediate weaponisation of a person's digitised features, proof-of-personhood intersects with performativity in structurally dangerous ways. Whether derived from highly specialised designs like Worldcoin's WorldID, or more commonplace mechanisms like Windows Hello and Apple's FaceID, proof-of-personhood schemes do not

[394] Josh Fruhlinger, "Opsec Examples: 6 Spectacular Operational Security Failures," *CSO Online*, 13 August 2021, https://www.csoonline.com/article/571107/opsec-examples-6-spectacular-operational-security-failures.html.

[395] Shurook S. Almohamade, John A. Clark and James Law, "Mimicry Attacks Against Behavioural-Based User Authentication for Human-Robot Interaction," in *Emerging Technologies for Authorization and Authentication* (ETAA 2021), Lecture Notes in Computer Science 13136 (Cham: Springer, 13 January 2022), 111-126, https://dl.acm.org/doi/10.1007/978-3-030-93747-8_8

[396] Dominic Forrest, "Challenges in Voice Biometrics: Vulnerabilities in the Age of Deepfakes," *ABA Banking Journal*, 15 February 2024, https://bankingjournal.aba.com/2024/02/challenges-in-voice-biometrics-vulnerabilities-in-the-age-of-deepfakes/.

[397] Federal Trade Commission, "FTC Proposes New Protections to Combat AI Impersonation of Individuals," press release, 15 February 2024, https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals.

[398] Lindsay Clark, "Rise of Deepfake Threats Means Biometric Security Measures Won't Be Enough," *The Register*, 1 February 2024, https://www.theregister.com/2024/02/01/deepfake_threat_biometrics/.

[399] Fred Heiding, Simon Lermen, Andrew Kao, Bruce Schneier and Arun Vishwanath, "Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects," arXiv pre-print, 30 November 2024, https://arxiv.org/abs/2412.00586.

[400] Marc Schmitt and Ivan Flechais, "Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing," arXiv preprint, 12 October 2023, https://arxiv.org/abs/2310.13715.

exist in isolation; They participate in, and reinforce, a broader cultural and infrastructural myth that devices can reliably verify humanness, and that biometric markers can be cleanly extracted from the complex social realities in which they operate. FaceID, fingerprint sensors, behavioural unlocks, device use, gait, iris scans – all are routinely deployed as de facto proofs of personhood, quietly reinforcing the narrative that smartphones are secure extensions of the self. This trust is unequivocally misplaced, as demonstrated by the endless arms race between malware vendors (the most notorious being Pegasus by the Israeli NSO Group) and a distributed network of vendors and security specialists. At the centre of it all is a fundamental truth that remains unchanged and unsolved for decades: If the device is compromised, nothing else matters.[401] To paraphrase Lily Hay Newman, writing for Wired: *"The age of assuming that iPhones and Android phones are safe out of the box is over."*[402]

Even in so-called privacy-preserving systems, such as those using zero-knowledge proofs or decentralised verification, the markers used to establish uniqueness (iris scans, gait, typing rhythm, device telemetry) are themselves extractable, replayable, or imitable given sufficient context.[403] [404] By 2025, pulling off this kind of operation barely requires technical skill: an attacker downloads a voice cloning tool from GitHub, feeds it a few seconds of source audio of a target's speech, and passes a banking voice ID system on the first try.[405] In other words, social engineering doesn't need to crack sophisticated cryptography; it needs only to mirror enough of the input assumptions to pass the unlock test.[406] *A successful social engineering attack relies on an attacker impersonating the performative self.*

Proof-of-personhood does not prevent this. It may even exacerbate it by embedding ambient trust into infrastructure. Once a system assumes that verification equals integrity, the surface of attack shifts away from perimeter and towards the assumption layer. The adversary walks through the front door, escorted by the very systems designed to keep them out, and the system's approval is visible to all other inter-operating systems and the humans overseeing them. With authentication in place, an attacker branded with the trust

[401] Sergiu Gatlan, "Apple Zero-Click iMessage Exploit Used to Infect iPhones with Spyware," *BleepingComputer*, 7 Sept 2023, https://www.bleepingcomputer.com/news/security/apple-zero-click-imessage-exploit-used-to-infect-iphones-with-spyware/.

[402] Lily Hay Newman, "A New Phone Scanner That Detects Spyware Has Already Found 7 Pegasus Infections," *Wired*, 4 Dec 2024, https://www.wired.com/story/iverify-spyware-detection-tool-nso-group-pegasus/.

[403] Darshika Jauhari et al., "Iris Presentation Attack: Assessing the Impact of Combining Vanadium Dioxide Films with Artificial Eyes," arXiv preprint, 21 Nov 2023, https://arxiv.org/abs/2311.12773.

[404] Bendik B. Mjaaland, Patrick Bours and Danilo Gligoroski, "Walk the Walk: Attacking Gait Biometrics by Imitation," in *Information Security* [ISC 2010], LNCS 6531 [Berlin: Springer, 2010], 361–380, https://link.springer.com/chapter/10.1007/978-3-642-18178-8_31.

[405] Joseph Cox, "How I Broke Into a Bank Account With an AI-Generated Voice," *Vice*, 23 Feb 2023, https://www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice/.

[406] Bruce Schneier, "Fooling a Voice Authentication System with an AI-Generated Voice," *Schneier on Security*, 1 Mar 2023, https://www.schneier.com/blog/archives/2023/03/fooling-a-voice-authentication-system-with-an-ai-generated-voice.html.

of a biometric identity system reinforces that trust with every interaction in the system. Detecting an intruder who has successfully developed a *parallel construction* of their target operates in a sort of limbo, undetectable yet visible, illegal yet impossible to easily prosecute.

~

Parallel construction of users in systems is not limited to fraud. Throughout the 20th century,police forces and intelligence services have been adept at harnessing the practice of parallel construction,[407] bypassing regulations that are geared towards limiting the sharing of personal information between law enforcement services to synthesise evidence and build narratives on persons of interest. As Jacob Ward notes in *The Loop*:

> *“DEA investigators might learn a drug trafficker’s identity from a confidential source, and then direct local police to follow that person’s car until it rolled through a stop sign or blew past the speed limit. The resulting traffic stop results in a search, the search finds the drugs, the case is made […].*
>
> *That practice has since expanded to become a means of using ethically dubious surveillance technology as the foundation of an arrest.”*[408]

This kind of attack exploits the performativity of identity rather than its content and is easily adapted to the digital context. It does not necessitate correlations of attributes to establish an identity, but rather extrapolates a behaviour from a personal data point in order to expand the surface of attacks from the digital to the material world. Much like with communication technology, as encryption of content became the norm, metadata surrounding the communication became an expedient medium to extrapolate criminal behaviours and relations. At its extreme of closed-circuit feedback loop, performativity ends up describing the normative influence exerted by predictive systems upon real-world behaviours, where predictions “wind up influencing the thing being predicted.”[409] In interviews, one participant reflected on how exploiting this behavioural extrapolation can be dangerously weaponised – even in mundane settings:

[407] Natasha Babazadeh, “Concealing Evidence: ‘Parallel Construction,’ Federal Investigations, and the Constitution,” Virginia Journal of Law & Technology 22, no. 1 [Autumn 2018]: 1-6, https://sog.unc.edu/sites/default/files/course_materials/Law%20Review%20Art%20on%20Parallel%20Construction.pdf.

[408] Jacob Ward, *The Loop: How Technology Is Creating a World Without Choices and How to Fight Back* [London: John Murray/Hachette UK, 25 January 2022]

[409] Ibid.

"In cybersecurity, there's one important tenet which is to see trust as what actually breaches cybersecurity measures. We've seen that already with digital identity weaponisation, right? What I would call, 'the performativity.'

I have one client who had to fight off a loan company, a telemarketer abusing their position of power. This telemarketer cyberbullied this client for half an hour. It was a contentious phone call, pushing my client to a state where she just lost her shit for a second: "You have to be more careful with people. You could drive someone to suicide." She just clapped back at this representative.

So it ends with her asking to talk to the telemarketer's supervisor. The latter felt like she was going to get in trouble. So she really escalated and made my client the problem. She went so far as to call the police in the area, saying that my client was a threat to herself or others, that she had attempted suicide. And my client was sectioned as a results, involuntarily committed and stripped of her rights as a human and as a citizen of the United States. She was placed into custody. I consider this to be similar to SWATTing."

Research participant
Researcher, specialist in generative AI and cybersecurity

What these corporate and domestic examples show is something beyond the ingenuity of bad actors: the structural failure of identity systems designed to privilege coherence over context. In both cases, the adversary succeeded by ignoring cryptographic and technical controls entirely, and choosing to exploit the assumption that personhood, once proven, is trustworthy; that signals delivered in the correct format should be acted upon. In the APT case, a daughter's photos – authentic, continuous, contextually believable – were weaponised to create trust. In the telemarketer case, distress is weaponised as affective proof of a situation gone wrong and fed into an institutional circuit pre-calibrated for intervention. In both cases, the attacker doesn't need access to credentials; All theyneed is to understand how to exploit the relevant control logic that governs how identity is interpreted within closed systems.

Systems of personhood, especially those that combine digital interaction with state or platform response, have little capacity to interpret context, emotion, or contested meaning. They operate on proxies: Performative affect becomes data, escalation becomes protocol, protocol becomes violence. Proof-of-personhood as implemented through biometric and behavioural markers reinforces this logic; training systems to treat certain patterns as "human," certain tones as credible and certain sequences of data as legitimate. **This is a true vulnerability of cybernetics in a time of information warfare**: inputs are normalised, interpreted, and acted upon without the full context, as much of it is invisible to the model.[410] The adversary, understanding the system's loop, introduces crafted input assembled from photos, metadata, speech and other data, at just the right time, with just the right resonance, to hijack the circuit. It's a man-in-the-middle attack, not on the network, but on the psychology of the trust model.[411] The proof is recontextualised both through the mistake of ambient trust *and* as an active cache of ammunition. In both cases, these systems function as designed.

In information security terms, *this is a failure of threat modelling* brought about by a limited imagination of defensive security. The system treats the user as the perimeter. Once they are verified, the internal logic unfolds automatically: access granted, escalation triggered, protocol executed. But both cases reveal that personhood, once weaponised, becomes an impossible to defend exploit vector. Just as malware often leverages legitimate system processes to execute unauthorised actions, social engineering attacks leverage legitimate identity performances to activate systemic responses.

Ruha Benjamin writes: *"I want us to think about how default settings in technology reflect default settings in society. What values are embedded in these systems? What types of people are valued or devalued through automated tools? Who is seen as a threat, and who is presumed safe?"*[412] In moments like these, the question of proof becomes far less important than the systems of belief into which it lands. A threat need not be real to be actionable, it need only be legible to the machine and credible to the institution. Such examples can flourish in a world of identity markers, and systems designed to authenticate against performative identity.[413]

~

The future of identity security cannot rely on hardened credentials alone. It must incorporate ambiguity, relational context, and the capacity to validate in non-replicable social ways. At the same time, the field of digital identity has not yet reckoned with the power of performativity in identity, where identity is something *beyond* a laissez-faire

[410] Michael C. Horowitz and Lauren Kahn, "Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts," *International Studies Quarterly* 68, no. 2 (June 2024): sqae020, published online 30 June 2023, https://arxiv.org/abs/2306.16507.

[411] Rosana Montañez, Edward Golob and Shouhuai Xu, "Human Cognition Through the Lens of Social Engineering Cyberattacks," *Frontiers in Psychology* 11 (30 September 2020): 1755, https://doi.org/10.3389/fpsyg.2020.01755.

[412] Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge: Polity Press, 2019).

[413] Rosana Montañez, Edward Golob and Shouhuai Xu, "Human Cognition Through the Lens of Social Engineering Cyberattacks," Frontiers in Psychology 11 (30 September 2020): 1755, https://doi.org/10.3389/fpsyg.2020.0175.

assemblage of serialised testimony; A complex product of contested 'meat-space' tensions, negotiated duties, interpersonal relations, and institutional clashes and contradiction. As Tamar Herzog notes in *Naming, Identifying and Authorizing Movement in Early Modern Spain and Spanish America*:

> *"Rather than constituting the person as the bearer of certain rights and duties, [identity documents and registries] indicated he may be thus. Rather than operating a transformation (making someone worthy of a certain treatment by the act of registering him or her), they recognized the validity of a change in status that had transpired beforehand, in fact sanctioning what oral negotiations had already consecrated. More often than not, rather than representing 'reality', registries gave proof of attempts by authorities [...] to control reality, attempts that were usually rejected [...]. [Written] registries always coexisted with an oral knowledge that either opposed or converged with them. How these two different registers coexisted (and perhaps coexist today) is a story we still need to explore."*[414]

Somewhere within the ongoing contest between the official registries of "the act of registering" and the vernacular knowledge of"what had transpired before," personhood is, for lack of a better term, "proved." Securing digital identity through MFA, ZKP or other SSI principles is only tackling the issue at its most technically simplistic level, for identity extends the surface of attack all the way through everyday performance: the daughter's holiday photos, the logistics of a drug deal, a union meeting, or the participation to a protest.

Werner Herzog (no relation) distinguishes between two types of truth: the "accountant's truth," which deals with factual accuracy, and the "ecstatic truth," which delves into a deeper, more profound understanding that transcends mere facts. He asserts that this deeper truth *"can be reached only through fabrication and imagination and stylisation."*[415] To confuse registration with recognition is to mistake the map for the territory. The field of digital identity continues to chase certainty through biometrics, device-bound attestations, cryptographic proofs, without recognising that identity is always already contested, contingent, and in motion. Identity lives not in the data, but in the frictions that data tries to overwrite; Systems of digital identity are designed to pursue the former, but it is the latter that governs how people actually live, relate, and resist.

[414] Tamar Herzog, "Naming, Identifying and Authorizing Movement in Early Modern Spain and Spanish America," in *Registration and Recognition: Documenting the Person in World History*, ed. Keith Breckenridge and Simon Szreter (Oxford: Oxford University Press for the British Academy, 2012), 191–210, https://academic.oup.com/british-academy-scholarship-online/book/13503/chapter/167014682.

[415] Werner Herzog, "On the Absolute, the Sublime, and Ecstatic Truth," trans. Moira Weigel, Arion 17, no. 3 (Winter 2010): 1–12, https://www.bu.edu/arion/files/2010/03/Herzog.pdf.

This ecstatic truth is not irrational. Beyond the model of identity, these are traits that allow a person to be understood despite inconsistent records, to be trusted in the absence of coherence, to exist beyond the machine's thresholds of legibility. The ecstatic truth is also precisely what gets erased when systems treat deviation as threat and pattern as virtue. It is this quiet, total, and unacknowledged erasure that adversaries exploit more effectively than any systems designer has ever defended against. The mission, endlessly stated, rarely achieved, is to secure the human. But identity cannot be secured, it is something to be entered, performed, misread, misused and sometimes even shattered. To enforce immutability is to enforce a brittle contradiction vulnerable to weaponised design.[416] ✳

[416] Cade Diehm, "On Weaponised Design," Our Data Our Selves, *Tactical Tech*, 16 February 2018, https://ourdataourselves.tacticaltech.org/posts/30-on-weaponised-design/.

8. Complex digital identity systems erode public trust

Key Points

- Complex digital identity systems deepen public mistrust by replacing accountability with protocol and dialogue with automation.
- Opaque infrastructure enables institutional evasion and fuels conspiratorial narratives across the political spectrum.
- Protocols encode power asymmetries that turn users into subjects and participation into compliance.
- Digital identity schemes delivered by foreign vendors or NGOs frequently bypass local governance, undermining legitimacy.
- History shows that identity is contested, constructed, and deeply political and attempts to standardise it through code provoke backlash.
- Mistrust in digital identity is not irrational; it reflects lived experiences of exclusion, opacity, and unaccountable control.

Like all digital technologies, digital identity relies on protocols, "a system of rules that allows two or more entities of a communications system to transmit information."[417] Indeed, the entirety of the digital identity initiative is built around the development and deployment of standards in the protocols governing personal attributes and identifying documents. While empowering exchange of information, protocols are as much spoken as unspoken, a necessary opaqueness meant to kickstart and facilitate the process of communication. It is within such opaque structures of information exchange that opportunities to cultivate public distrust reside.

This research finds that, as these are being weaponised, and as technology reaches ever further into societies, these obfuscations have far reaching and underappreciated potential consequences.

~

As digital platforms and services take over responsibilities once held by public institutions, they introduce new layers of opacity. Decisions that affect people's access to welfare, credit, healthcare, or participation are often made by systems whose internal logic is inaccessible, even to those administering them. When questions are asked about why a claim was denied, why a vote didn't register, why someone was flagged, there are few answers. Often, there's simply no one to ask.

Warranted or not, this distrust can in turn be embodied in intense and radical forms of contest, from the most legitimate[418] to the most pernicious. The absence of accountability is

[417] Wikipedia, s.v. "Communication protocol," last modified 25 May 2025, https://en.wikipedia.org/wiki/Communication_protocol [accessed 13 June 2025].

[418] Heather Vogell, with data analysis by Haru Coryne and Ryan Little, "Rent Going Up? One Company's Algorithm Could Be Why," *ProPublica*, 15 October 2022, https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent.

distrust sparked from confusion, accelerated by the opaque, top-down social paternalism of digital identity. With little power to affect the immediate, and no visibility of the systems that immediately influence their lives, imagination and speculation fills the void and becomes truth over time. Sometimes that takes the form of critique: demands for oversight, transparency, or reform. But often, especially when such systems are tightly coupled to a Neoliberal apparatus considered unjust or uncaring, suspicion becomes its own structure, and speculation hardens.

In the US, this takes the form of the manipulation of social media data during the Trump campaign. The obsessive retrial of Clinton's private email server. QAnon's metastasis into a participatory fiction about unseen elites. In Brazil, Bolsonaro's use of WhatsApp and Telegram to construct an anti-institutional narrative scaffold. In Venezuela, Nicolás Maduro's use of biometric ID in the CLAP food distribution system, tying aid to political loyalty. In India, Aadhaar-linked subsidies gradually transformed into a mechanism of exclusion; when new agricultural laws threatened to extend this automated precarity to land and trade, the farmers' protests erupted against deregulation, fuelled by a deepening frustration of being made illegible by systems they could not contest.

Across Europe, the same pattern repeats in different keys. Spain's digital ID regime fractured under the weight of Catalan independence claims. France advanced a proposal to tie biometric data to welfare access. In the Netherlands, an algorithmic tax fraud system falsely profiled and penalised thousands of ethnic minority families. Hungary expanded its identity governance apparatus to marginalise Roma and LGBTQ+ communities. In Israel, biometric infrastructure deepened the surveillance and control of Palestinians. The Schengen regime, once a symbol of post-national mobility, quietly collapsed into fragmented biometric borders during the pandemic. And far-right parties across the EU increasingly rally around digital ID refusal, platform mistrust, and the restoration of analogue control – less as nostalgia than as strategy.

None of these are isolated events. They are variations on a broader pattern: the political consequences of outsourcing governance and recognition to systems that do not explain themselves. Civil digitisation, far from neutral, acts as an accelerant that widens the gap between governance and legibility. What emerges is an unrecognisable kind of policy failure rooted in interpretive vacuum, where every back end decision becomes a opportunity to theorise and every unexplained denial or approval becomes a story. Digital identity, correctly recognised by the citizenry as the conduit for the unaccountable imposed will, becomes the terrain on which that question is endlessly contested.

~

Counter-productively, much of the forays into digital identity is geared towards dissipating the obfuscation that reside *on the user-consumer side.* Digital identity strives to fix much of the perceived issues of pseudonymity and anonymity that have been magnified with the development of social media, especially with regards to identity fraud. Left unresolved, this type of fraud is easily placed entirely at the feet of users, and would immediately destroy any attempt at building Web 3, with its intensification of user-generated revenue streams and assetisation. Yet this does nothing to combat the obfuscation provided to the side of incumbent power.

On the contrary, it accentuates it. As discussed in the previous findings, our research shows that the monopolisation and concentration of power associated with the the necessary outlays of financial and political capital will only accentuate the differential between users of digital identity and the service providers, as it will allow the latter to dictate the terms of the protocols. This is a foundational and structural concern. Moreover, governmental or supra-governmental initiatives, like the EU DC4EU, do not exist in a vacuum, but side by side with the creep of social media platform into personal and biometric information,[419] addictive game platforms' foray in identification technology,[420] or weaponisable menstrual cycle tracking apps.[421] To ignore that these cases coexist side-by-side with the lofty ideals of new-generation identity systems, or indeed could be expected to interact with them,[422] is an error legislators and government officials cannot afford to make. Just like the dot-com bubble harkened the concentration of the web into fewer hands, and the Web 2.0 centralised the avenues of information, so too digital identity can be expected to consolidate power for incumbent actors, further fuelling public distrust in digitally mediated processes.

Electoral systems are an especially potent site of this distrust. As voting infrastructure becomes entangled with digital identity verification through e-voting platforms, biometric check-ins, or digital voter rolls, its opacity becomes politically explosive. Allegations of fraud no longer require evidence of tampering; they require only the appearance of complexity. The very protocols meant to secure the vote begin to look like arcane

[419] Emma Roth, "X Wants Permission to Start Collecting Your Biometric Data and Employment History," *The Verge*, 31 August 2023, https://www.theverge.com/2023/8/31/23853618/x-privacy-policy-update-biometrics-job-history.

[420] Guilded, "Update to Guilded Login Requirements," *Guilded Blog*, 31 May 2024, https://www.guilded.gg/blog/update-to-guilded-login-requirements.

[421] Anna Merlan, "Peter Thiel's Investment Firm Is Backing a Menstrual Cycle-Focused 'Femtech' Company," *Vice*, 6 September 2022, https://www.vice.com/en/article/peter-thiels-investment-firm-is-backing-a-menstrual-cycle-focused-femtech-company/.

[422] The Wolfsberg Group. "The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity," 8 July 2024, https://db.wolfsberg-group.org/assets/e3d83d2f-fad9-46d2-b5a9-3cf4e932f53f/Wolfsberg%20Group%20Statement%20on%20Effective%20Monitoring%20for%20Suspicious%20Activity.pdf

gatekeeping mechanisms. In the 2024 U.S. election cycle, for example, conspiracy theorists did not need to breach the system. They only needed to tell a compelling story about its black-box nature, peppered with enough technical terminology to sound plausible. Digital identity, in this context, becomes narrative fuel.

This strategy is not new, digital identity as a so-called pillar of mass control is a staple conspiracy theory derived from the very real Nazi abuse of digital identity systems for control and extermination. In modern contexts, these narratives have are the fertilizer that nourish the Neo-reactionary far-right movements across the globe, which have increasingly framed digital identity as a tool of population control or globalist governance. Whether cast as biometric overreach or the infrastructure of a "new world order," digital identity systems provide the perfect antagonist: invisible, bureaucratic, and selectively punitive. While these views are often conspiratorial, they are not delusional. They are built from real histories of exclusion, opaque design, and the casual arrogance of systems builders who assume that trust can be engineered without dialogue.

Beyond the Western context, policy failures and conniving between governments and the private sector have already seeded distrust, such as in the Democratic Republic of Congo, Mozambique and Uganda.[423] [424] Historically, successful identity schemes have been endogenous policies established and enforced from within a given polity. Buganda/Uganda offers a fascinating early example of such a program before its colonisation by Western powers.[425] While this does not preclude abuse and exploitation, these policies nevertheless originated from a sense of shared destiny within a body politic, rather than a pure biopolitical effort mediated by foreign privatised solutions. As Dominique Mashall noted on the worldwide movement for birth registration:

> *"[The] movement to promote birth registration as a universal right for children in the interwar USA and Africa and on the post-war international stage shows that contemporary UN and NGO initiatives are heir to a complex prior political history in the twentieth century [from colonial custom to the 'calculative practices' of self-interest influenced by neoliberalism]. [There] are few parts in the world, even in those countries where registration systems are currently lacking, where identity registration systems have*

[423] Beatriz Ramalho da Silva and Tomas Statius, "Africa's Identity Crisis," *The Continent*, 13 August 2024, https://continent.substack.com/p/africas-identity-crisis.

[424] Olivia Solon et al., "False Promise of Biometrics," *Lighthouse Reports*, 5 June 2024, https://www.lighthousereports.com/investigation/false-promise-of-biometrics/.

[425] Dominique Marshall, "Birth Registration and the Promotion of Children's Rights in the Interwar Years: The Save the Children International Union's Conference on the African Child and Herbert Hoover's American Child Health Association," in *Registration and Recognition: Documenting the Person in World History*, ed. Keith Breckenridge and Simon Szreter (Oxford: Oxford University Press for the British Academy, 2012),

not in fact been already promoted and in many cases temporarily established [...]. The current international movement to promote registration at birth could benefit from paying close attention to its precursors in this rich history [...].”[426]

Endogenous identity systems, however flawed, tend to emerge within a structural framework of negotiated accountability, and are shaped by the logics of local governance, social relation, and political rupture. They can be protested, boycotted, reformed or negotiated. In contrast, contemporary digital identity schemes are often delivered as turnkey solutions by NGOs, private consortia, or supranational private/state cooperative initiatives. These systems present themselves as neutral infrastructure but are, in fact, saturated with ideological assumptions: about what counts as a person, what data is valuable, what behaviours are legitimate, what institutions can be trusted. The McKinsey Global Institute highlights that while digital IDs can drive economic growth, their implementation often lacks consideration of local contexts and governance structures, leading to potential issues of exclusion and mistrust.[427] Truer words have never been spoken from the mouth of the beast itself.

Whereas such technological claims to neutrality can be easily disputed and dismantled, the protocols of digital identity are better understood as *frozen politics*; Once embedded, they are difficult to modify or contest, local populations become users (not constituents), participation becomes compliance. When these systems fail – *and they will* – the accountability mechanisms are unclear or non-existent. Therefore: **people do not distrust digital identity systems because they are irrational or resistant to change. People distrust them because they cannot shape them.**

In contrast, contemporary digital identity schemes are often introduced as turnkey solutions by NGOs, private consortia, or supranational initiatives. These systems present themselves as neutral infrastructure but are imbued with ideological assumptions about personhood, data valuation, and institutional trustworthiness. Today, a whole host of disparate identity schemes are tacked on populations through the effort of the private sector or NGOs. Some of these efforts are already under investigation for corporate criminality.[428] The promoters of such programs forget, as Chris Wiggins and Matthew L. Hones remind us, that *“[f]orms of recording that we now take for granted, such as the birth*

[426] Ibid.

[427] Olivia White, Anu Madgavkar, James Manyika, et al., “Digital Identification: A Key to Inclusive Growth.” *McKinsey Global Institute*, 17 April 2019, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

[428] Yann Philippin, “Gemalto est visé par une vaste enquête pour corruption en Afrique,” *Mediapart*, 7 February 2023, https://www.mediapart.fr/journal/international/070223/gemalto-est-vise-par-une-vaste-enquete-pour-corruption-en-afrique.

certificate, made people into data in an unprecedented way. And they did so only through tremendous, consequential, contested work, what historian Wangui Muigai describes as the "interactions, confrontations, and disputes over how individual people should be accounted for and the labour involved in constructing and documenting those identities."[429]

~

From the World Economic Forum to the Red Cross to the United Nations to the architects of the Estonian *Tiigrihüpe* (Tiger Leap), the contemporary proponents of digital identity frequently overlook this history of friction, contingency, and deeply political work. It is a mistake to think of identity as given,awarded, inherent – identity is always constructed, always situated, and often contested through interpersonal and institutional struggle. What digital identity protocols attempt to do is bypass this labour by encoding identity as a universal, legible, and self-evident structure. But this is a fantasy; The more technical the protocol, the more political its exclusions.

As a result, protocols erase the negotiations they claim to standardise. They formalise identity as a system of authorisation with the rhetoric of shared social recognition. In the context of democratic systems, this amounts to a series of systems designed to be parsed by machines, implemented by foreign vendors, and enforced by institutions with little accountability. Increasingly (and frequently by vendors' own admissions) these identity infrastructures are deployed in domains where contest should be protected: access to elections, asylum procedures, humanitarian aid. The same architecture used to provision welfare is used to deny movement. The same biometric profile used to vote can be used to exclude; Identity becomes an access token that can be revoked.

To frame this as a technical problem is to misunderstand its foundation. Identity infrastructures are not failing because they are insufficiently precise, they are failing because they refuse to account for the political work they are built upon. And the result is not just exclusion. It is resentment, instability, and eventually, crisis.

What Muigai describes as *"interactions, confrontations and disputes"* stand in stark contrast to the idealised and sanitised discourse that surrounds digital identity. Proof-of-personhood, like other protocols of recognition, attempts to resolve that mess through technical means. But what it produces instead is a zone of contest: a heterotopia where competing logics of verification, control, refusal, and survival collide.

[429] Chris Wiggins and Matthew L. Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. W. W. Norton & Company, 2023.

Such sites illuminate the true function of protocol as a mechanism of power, calibrated to soothe the powerful and sort the rest. When these systems fail to account for the political labour that identity requires, they produce both exclusion *and* disillusionment. When that disillusionment festers among voters, migrants, protestors, or patients, it nevertheless does not remain quiet. It metastasises into conspiracy, unrest, and paranoia. The result, when combined with the other visible pitfalls of digital identity, is a tearing of the social fabric and systemic crisis that no cryptographic ledger or biometric ledger can contain. ✳

9. Digital identity creates state sovereignty risk

As societies digitise, they do so primarily to manage citizens, land, infrastructure, and operations. Management demands representation. In digitised governance, digital identity becomes the canonical form of that representation: a system that recognises, tracks, authenticates, and authorises individuals and entities. It defines how power is exercised and where sovereignty is asserted. But the interface – where most policy and public debate ends – is only the surface. Beneath every national identity app lies a brittle, externalised foundation: supply chains, cloud dependencies, software dependencies, hardware constraints, jurisdictional overlaps, platform gatekeepers, and transnational standards, all operating beyond the reach of the state. Identity flows across fibre owned by foreign firms, depends on hardware regulated abroad, and is verified through infrastructure governed by unaccountable external actors. Whether through ideology, expedience or design, systems that ignore these conditions cede control to unseen actors. Sovereignty cannot be asserted through infrastructure controlled elsewhere.

Key Points

- Digital identity reshapes sovereignty: core systems depend on foreign platforms, placing states in technical subordination.
- *Kill switch sovereignty* emerges when identity infrastructure can be paused or surveiled by external actors, undermining autonomy.
- Jurisdictional overflow entangles ID data in conflicting legal regimes, enabling extraterritorial influence and control.
- *Programmable personhood* encodes civic status in software, making access to rights revocable by code or contract.
- From Aadhaar to Diia, digital ID systems often embed soft power and coercion beneath promises of inclusion.
- Self-sovereign and decentralised identity systems replicate the same risks when built atop foreign-controlled infrastructure or governance-by-protocol.
- Sovereignty compromise is inherent to the digital identity stack through extractive, postcolonial tech supply chains comprised of rare earths, cloud monopolies, and outsourced control.
- Sovereignty requires infrastructural autonomy. Without it, identity becomes programmable by others.

This is a risk that is already being realised. Our research confirms that digital identity systems are increasingly deployed to consolidate leverage, under the umbrella of inclusion and efficiency. Through interviews with on-the-ground participants reckoning with sovereignty risk in unstable state contexts, and in examples from the wider world, **we argue that the deployment of digital identity systems consolidate leverage and coercion despite promises of inclusion.** The outcome of a successful society-wide digital identity is the instalment of a new soft power and coercive capability that quietly redraw the boundaries of national autonomy. This is true whether administered through Apple/Google wallets, Web3 identity systems, digital welfare platforms, PGP keys, or countless other examples, and is also true both historically and in the present geo-politicking of 2025.

When prescribed beyond the Western context – where many of these designs originate – digital identity standards become deeply colonial. Cross-border mandates embed assumptions about trust, risk, and governance that do not reflect lived conditions, embedding specific assumptions about privacy, centralisation, and operational continuity that routinely fail under duress. Like the green energy transition, which depends on toxic rare metal extraction from post-colonised regions,[430] digital identity hastens global dependency on brittle, extractive systems. The aftermaths of unintended consequence of digital identity are often treated as exceptional rather than systemic, despite being the inevitable result of outsourced infrastructure. While crude data nationalism risks fracturing the global internet into walled gardens, total infrastructural dependence delivers power to external states and corporations by default. **A sovereignty that can be paused, surveiled, or revoked at the discretion of another state is no sovereignty at all.**[431]

~

Modern states increasingly depend on private digital platforms to run critical identity and data services, a dependency that can erode traditional sovereignty. Unlike physical borders or state-run utilities, digital identity infrastructure often resides in cloud servers owned by tech giants. This creates a scenario where a nation’s core databases and authentication services may be hosted on foreign soil or managed by foreign corporations. As an example, cloud computing behemoths like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform now host government platforms worldwide. Over 97% of Germany’s leading companies rely on cloud services – most using AWS, Azure, or Google – and many governments from Britain to Australia also entrust critical functions to these U.S.-based clouds..[432] By 2024, U.S. cloud providers dominated 70% of the €70 billion European cloud infrastructure market.[433] Such reliance means that the legal and operational control over data can extend beyond the nation’s own jurisdiction, ceding a degree of sovereignty to platform providers.

[430] Guillaume Pitron, *La guerre des métaux rares: La face cachée de la transition énergétique et numérique* [Paris: Les Liens qui Libèrent, 2018], https://shs.cairn.info/revue-projet-2018-2-page-90?lang=fr.

[431] Borja Larrumbide and Daniel Fuertes, “Customer Checklist for eIDAS Regulation Now Available.” *AWS Security Blog*, 9 May 2023, https://aws.amazon.com/blogs/security/customer-checklist-for-eidas-regulation-now-available/.

[432] Rafal Rohozinski, “The Brutalist Web.” *Centre for International Governance Innovation*, 21 March 2025, https://www.cigionline.org/articles/the-brutalist-web/.

[433] Synergy Research Group, “European Cloud Providers’ Local Market Share Now Holds Steady at 15%,” *Synergy Research Group Newsroom,* 24 July 2025, https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15.

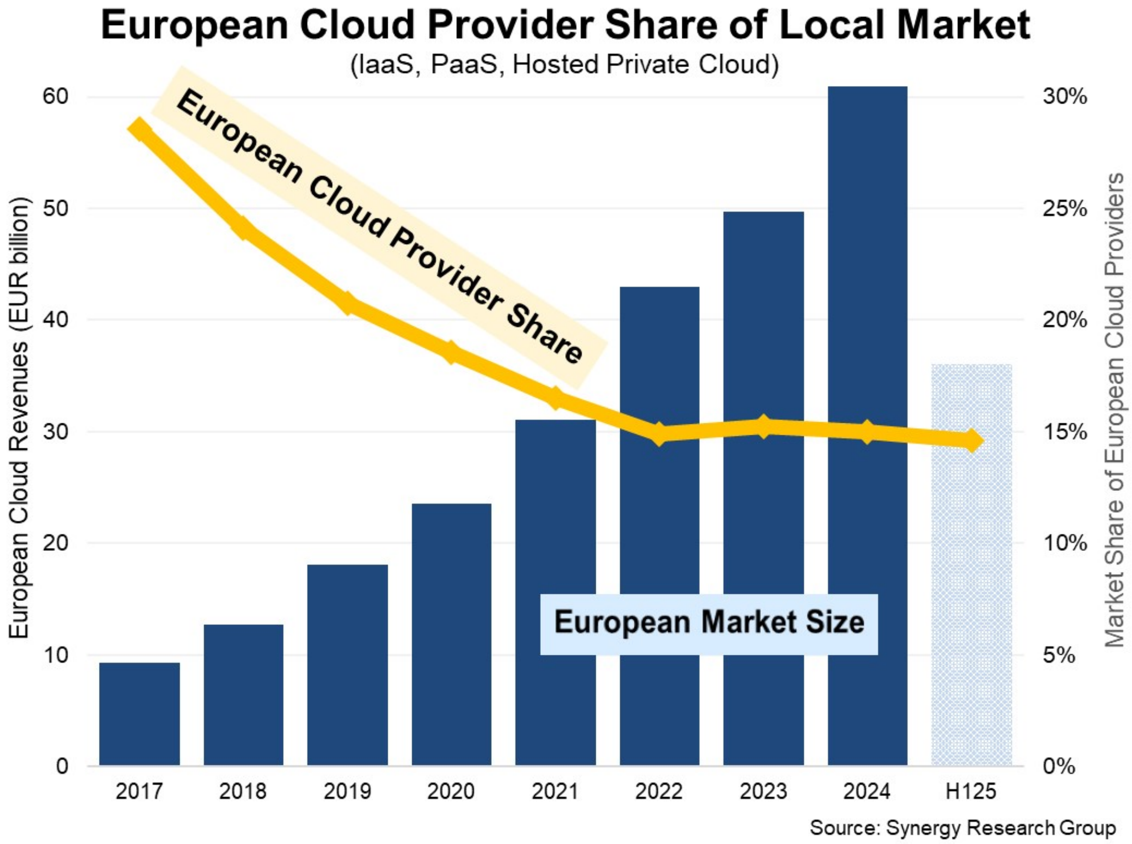


Figure: Marketshare of European cloud vendors compared to revenue from European Cloud customers.[434]

Under President Donald Trump's renewed "America First" doctrine, introduced in 2025, U.S. dominance in digital infrastructure has been more openly wielded as a geopolitical lever. Allies – particularly the European Union – have been jolted by the realisation that their dependence on American tech might be used against them.[435] A stark illustration came when an unnamed U.S. negotiator allegedly threatened Ukraine: "either sign the minerals deal, or we'll shut down Starlink."[436] This ultimatum – essentially a kill switch threat–demonstrated how swiftly digital lifelines can become leverage. This episode reveals a new paradigm of kill switch sovereignty: if key digital services underpinning a state (communications, clouds, identity systems) are controlled elsewhere, those external powers hold an effective "switch" to diminish a state's autonomous functions. Digital dependency thus translates into strategic vulnerability, where core aspects of governance (from connectivity to public records) are subject to foreign influence or coercion.

[434] Synergy Research Group, "European Cloud Providers' Local Market Share Now Holds Steady at 15%," *Synergy Research Group Newsroom*, 24 July 2025, https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15.

[435] Bert Hubert, "It Is No Longer Safe to Move Our Governments and Societies to US Clouds." Bert Hubert's Writings, 23 February 2025, https://berthub.eu/articles/posts/you-can-no-longer-base-your-government-and-society-on-us-clouds/.

[436] Abbey Fenbert, "US Threatens to Shut Off Starlink if Ukraine Won't Sign Minerals Deal, Sources Tell Reuters." *Kyiv Independent*, 22 February 2025, https://kyivindependent.com/us-threatens-to-shut-off-starlink-if-ukraine-wont-sign-minerals-deal-sources-tell-reuters/.

Historically, control over infrastructure has been a means to exert influence – akin to how control over oil or canals shaped 20th-century geopolitics. Today's equivalent is control over digital identity platforms and data flows. Scholars liken American cloud providers to the "United Fruits" of the digital era, recalling the fruit companies that once dictated Central American politics. In lieu of plantations and railroads, the contested territory is now the cloud and internet backbone. When nearly all authentication of citizens or storage of national biometric registers run through foreign servers, sovereignty is partially outsourced. This restructuring of power raises urgent questions: Can a state truly be sovereign if it cannot control the on/off switch of its own citizen databases? Is reliance on another country's tech firms creating a form of jurisdictional overflow, where U.S. laws and interests effectively overflow into other jurisdictions via digital means?

Shockingly, the European Union has only recently recognised this challenge and fears the consequences of platform dependency. Trump's return to office in 2025 amplified these worries, prompting European policymakers to scramble for greater digital autonomy. As one expert noted, there is "huge appetite in Europe to de-risk or decouple the over-dependence on U.S. tech companies" amid concern that these technologies "could be weaponised against European interests".[437] In March 2025, the Dutch Parliament even approved eight motions instructing their government to reduce reliance on U.S. tech firms, following an open letter by over 100 organisations warning that the status quo imposes "security and reliability risks".[438] This momentum reflects a broader movement to reclaim digital sovereignty: Europe is effectively trying to mitigate the kill switch risk by diversifying or localising critical infrastructure.

~

At the same time as a newly belligerent dependency rises from Washington, the European Union continues to push the The erosion of sovereignty across the EU, where digital credentials are quietly hosted on American cloud infrastructure, is mirrored by a parallel disempowerment of resource-rich states in the Global South,[439] [440] where international organisations, foreign corporations, or tech-exporting nations play a significant role in

[437] Anna Desmarais, "Can the US Turn Off European Weapons? Experts Weigh In on 'Kill Switch' Fears," *Euronews Next*, 13 March 2025, https://www.euronews.com/next/2025/03/13/can-the-us-turn-off-european-weapons-experts-weigh-in-on-kill-switch-fears.

[438] Toby Sterling, "Dutch parliament calls for end to dependence on US software companies," *Reuters*, 19 March 2025, https://www.reuters.com/world/europe/dutch-parliament-calls-end-reliance-us-software-2025-03-18/.

[439] Maeve Campbell, "In Pictures: South America's 'Lithium Fields' Reveal the Dark Side of Our Electric Future." *Euronews Green*, 1 February 2022, https://www.euronews.com/green/2022/02/01/south-america-s-lithium-fields-reveal-the-dark-side-of-our-electric-future.

[440] International Energy Agency, *Global Critical Minerals Outloo*k 2024 (Paris: IEA, 2024), https://www.iea.org/reports/global-critical-minerals-outlook-2024.

identity programs.[441] The results can both empower and exclude, and in many cases, external players gain leverage that challenges or reshapes state sovereignty.

In the late 2010s, Kenya introduced the Huduma Namba, a digital ID intended to unify personal data for easier access to government services. In 2021, Kenya's High Court in declared Huduma Namba illegal for violating the Data Protection Act by collecting intrusive data (like DNA and GPS coordinates) without adequate safeguards. The court noted that such sensitive data, if breached or misused, posed significant risks to citizens' privacy and rights.[442] Despite this setback, the Kenyan government launched a new digital ID project (sometimes referred to as Maisha Namba) to replace Huduma, signifying the state's strong drive toward digitisation. Under President William Ruto, Kenya aims to have all citizens digitally identified, with the goal of moving 80% of services online.[443]

To achieve this ambitious goal, the Kenyan government forged partnerships with foreign tech and finance firms. For instance, Mastercard developed a smart ID card for Kenya that doubles as a payment card, enabling citizens to pay for government services and receive welfare benefits through the same system.[444] While this promises efficiency and financial inclusion, it also means a multinational corporation is entwined deeply in the country's identity infrastructure. Mastercard's involvement is framed as philanthropy and innovation and the company pledges publicly to provide digital identity to 100 million people in Africa, raising questions about data ownership and surveillance and Kenyan state autonomy. What does it mean for a system's designs and endpoints to be wholly controlled by an external party?

Kenya's case exemplifies a common pattern: the fusion of identity with financial services via public–private partnerships creates asymmetric power structures already explored in this report. But there is also a physicality to the power asymmetry, in the design, administration and issuance of the technology itself. Citizens may be required to use these digital IDs to receive essential services, effectively ceding part of a state's agency to third parties as a condition of access. As one study of Tanzania's digital ID system found, even

[441] Cour administrative d'appel de Bordeaux, "Projet « Montagne d'or » en Guyane : les concessions minières ne seront pas prolongées," 26 November 2024, https://bordeaux.cour-administrative-appel.fr/decisions-de-justice/dernieres-decisions/projet-montagne-d-or-en-guyane-les-concessions-minieres-ne-seront-pas-prolongees.

[442] Privacy International, "Data Protection Impact Assessments and ID Systems: The 2021 Kenyan Ruling on Huduma Namba," *Privacy International*, 27 January 2022, https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

[443] "President Ruto Says 80 pc of Govt Services on Digital Platforms." *Capital News [Kenya]*, 22 April 2024. https://www.capitalfm.co.ke/news/2024/04/president-ruto-says-80pc-of-govt-services-on-digital-platforms/.

[444] Mastercard, "Huduma Card Delivers Cashless Efficiency, Powered by Mastercard Technology," press release, 8 February 2017, archived at Internet Archive Wayback Machine [capture 9 March 2017], https://web.archive.org/web/20170309061621/https://newsroom.mastercard.com/mea/press-releases/huduma-card-delivers-cashless-efficiency-powered-by-mastercard-technology/.

with broad adoption, the system carried "design potential to exclude" and forced citizens to negotiate with service providers and invest their own effort to protect their digital identities.[445]

India's Aadhaar program similarly straddles a line between empowerment and external influence. In 2010, India's UIDAI (Unique Identification Authority) awarded contracts to U.S. and French companies (including L-1 Identity Solutions, now Idemia, and Accenture) to build Aadhaar's biometric matching systems.[446] Critics argue this not only gave foreign firms access to Indian citizens' personal and biometric data, but also created national security risks. Petitions filed in Indian courts questioned whether citizens ever consented to their data being shared with foreign entities and pointed out links between those firms and foreign intelligence agencies.[447]

While the government maintains that data is protected, the perception of external access to a sovereign database has spurred debate about digital self-reliance. Moreover, Aadhaar has been used as a case study in how an ID can become de facto mandatory: services like banking,[448] mobile phones, and even school exams[449] started requiring Aadhaar, effectively programming personhood into a digital token – if you aren't in the database, you struggle to exist in society. The flip side is that being in the database means being constantly legible to the state (and possibly its contractors). This all-or-nothing dynamic of digital identity – either you are recognised by the digital system and granted rights, or you are invisible and denied – is a fundamental restructuring of sovereignty at the individual level, often described as the trade-off between inclusion and surveillance.

Another striking case is Venezuela's *Carnet de la Patria* ("Fatherland Card") Introduced by the Venezuelan government towards the end of the 2010s, the identity system's implementation involved foreign technology that carry geopolitical undertones. The Carnet is a smart ID card introduced under President Nicolás Maduro, intended to centralise data

[445] Patricia Boshe, *Digital Identity in Tanzania* (Cape Town: Research ICT Africa/CIS, October 2021), 49-50, https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Tanzania_31.10.21.pdf.

[446] Kirtika Suneja, "UID Selects Accenture, Satyam, L-1 for Biometrics Contract," *Business Standard*, 29 July 2010, https://www.business-standard.com/article/technology/uid-selects-accenture-satyam-l-1-for-biometrics-contract-110072900084_1.html.

[447] Vallari Sanzgiri, "Petition Against UIDAI Sharing Aadhaar Data With Foreign Companies," *Medianama*, 22 November 2022, https://www.medianama.com/2022/11/223-petition-against-uidai-aadhaar-data-sharing-foreign-companies/.

[448] Reserve Bank of India, "RBI Clarifies That Linking Aadhaar Number to Bank Account Is Mandatory," Press Release, 21 October 2017, https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=42024

[449] Central Board of Secondary Education (CBSE), "CBSE Students Must Submit Aadhaar Number for Registration," *Circular*, 15 May 2017, https://www.cbse.gov.in/cbsenew/Examination_Circular/2017/28_CIRCULAR.pdf.

on citizens and manage access to social programs. Behind it was Chinese telecom giant ZTE, hired in 2017 to build the database and card system.[450]

Carnet holds a QR code linking to a vast repository of information, including personal data, and political affiliation via financial transactions to political entities. The card is increasingly required to receive subsidised food, fuel, and healthcare, and critics – including a Reuters investigation – revealed that the system was directly inspired by China's social monitoring techniques.

The result is so obvious it would be wholly unsurprising if it wasn't so nefarious: Carnet is used to track and reward or penalise behaviour pulled from its data set.[451] For example, leading up to elections, Venezuelans reported that scanners were set up to check Carnets at voting stations, effectively allowing the ruling party to monitor who voted, or even whether they voted "correctly", according to allegations.[452] The Carnet exemplifies programmable personhood: it's a state-issued digital identity that can be programmed to dispense benefits or inflict exclusion based on one's compliance or loyalty.

The public/private partnerships embedded in almost all modern implementations of digital identity allows for an opportunity to cultivate 'hard' power and social control by the internal state, along with soft power externally, as shown in the examples of India and Venezuela. The presence of Chinese, American, or other foreign technologies in a nation's identity scheme often reflects larger geopolitical alignments that go completely unspoken by decision-makers.

~

Digital identity systems become especially consequential in conflict zones or amidst state crises. In these environments, identity can determine safety: who is entitled to cross a border, receive aid, or avoid suspicion. Conversely, identity data falling into the wrong hands can spell persecution. Thus, controlling identity systems becomes a form of power for both state and non-state actors.

During the 2022 Russian invasion of Ukraine, digital identity took on wartime importance. The nation's *Diia* app – which stored citizens' IDs and certificates and allowed them to

[450] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters*, 14 November 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.

[451] LatinAmerican Post, "The Venezuelan ID: The New Citizen Pain," *LatinAmerican Post*, 25 July 2018, https://latinamericanpost.com/americas/the-venezuelan-id-the-new-citizen-pain/.

[452] Alex Kliment, "Votes for Butter: Rigging an Election in Venezuela," *Axios*, 28 March 2018, https://www.axios.com/2018/03/28/maduro-rigging-election-using-food-votes.

interact with the state, became a key interface for war support.[453] Fearing that Russian forces could seize national databases, Ukrainian authorities made a dramatic decision early in the war: destroy localised datasets to prevent abuse by occupiers. This protective measure comes at a sovereignty cost. The highly portable data, now destroyed, causes significant bottlenecks in a system designed with the assumption that such data will remain, and that the destruction of a government data set is something beyond an edge case. For Ukraine, officials had to turn to commercial providers to both govern the embattled country and support millions of displaced Ukrainians,[454] meaning that as a consequence of the war, Ukraine's government could only recognise its diaspora through systems provided by external companies, effectively outsourcing a core sovereign function in a moment of crisis.

Meanwhile, both sides in the war weaponised identity data. Ukrainian hacktivists doxxed Russian soldiers – dumping their personal data online – as a tactic of psychological warfare.[455] Russia, for its part, likely sought any Ukrainian databases to identify resistance networks or target individuals.[456] The conflict saw SIM card registration data and other civilian identities reportedly used to profile and locate targets.[457] [458] In war, controlling identity infrastructure (or denying it to the enemy) becomes as critical as controlling bridges or airspace. Digital identity easily becomes a kill list if exploited by an enemy, similar to paper copies of census data in the 20th century. Unlike the 20th century, modern digital identity systems are ephemeral and portable; Once popped, their contents can be syphoned invisibly to anywhere in the world.

The Ukraine case exemplifies how digital identity intersects with hard power: it can aid in mobilising defence (verifying volunteers, delivering services to refugees) but can also amplify vulnerabilities, forcing a state to trust foreign tech under dire conditions or risk massive data breaches with lethal consequences.

[453] United Nations Development Programme, "Updated e-Service in Diia: IDPs Can Now Apply for Aid for the Whole Family," *UNDP Ukraine*, 9 April 2024, https://www.undp.org/ukraine/press-releases/updated-e-service-diia-idps-can-now-apply-aid-whole-family.

[454] Amazon Staff, "Safeguarding Ukraine's Data: The Critical Role of Cloud during War," *About Amazon*, 9 June 2022; updated 14 April 2023, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

[455] Matt Burgess, "Russia Is Leaking Data Like a Sieve," *Wired*, 13 April 2022, https://www.wired.com/story/russia-ukraine-data/.

[456] Belkis Wille, et al., "'We Had No Choice': 'Filtration' and the Crime of Forcibly Transferring Ukrainian Civilians to Russia," *Human Rights Watch*, 1 September 2022. https://www.hrw.org/report/2022/09/01/we-had-no-choice/filtration-and-crime-forcibly-transferring-ukrainian-civilians.

[457] Kieran Devine, "Mobile Networks Being Weaponised to Target Troops on Both Sides," *Sky News*, 4 January 2023, https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595.

[458] Eric Priezkalns, How Russia and Ukraine Tracks Mobile Phones on the Battlefield, *Commsrisk*, 26 February 2024, https://commsrisk.com/how-russia-and-ukraine-tracks-mobile-phones-on-the-battlefield/.

In other crisis zones, identity is often the first casualty and the first thing rebuilt – sometimes with foreign help that later translates into influence. After the collapse of government authority in places like Libya or Yemen, citizens can become "legally invisible" as records fragment or are lost. International agencies might step in to document people (issuing refugee identities, for example). While life-saving, these external systems can overshadow or replace national ones.

For instance, in Syria and later for Syrian refugees, the UNHCR issued refugee identity cards that, in practice, became more important than any Syrian documents. These cards could be seen as a form of "transitional sovereignty" by the UN – defining who a person is for purposes of aid and resettlement, separate from their country of origin's control. Conditional recognition comes in when those who lack the right digital credentials might not be recognised at all.

Finally, digital identity can become entrenched through internal crisis, where a government opts to use digital identity systems to consolidate control in a post-crisis rationalization. After putting down a rebellion or coming out of a state of emergency, a regime might introduce a new identity system "to improve security" – in effect solidifying surveillance measures normalized during the crisis. For example, after the COVID-19 pandemic, some countries made temporary digital health passes into broader digital identity infrastructure,[459] something the European Commission and the World Health Organization are actively pursuing despite the ongoing fracture of global pandemic cooperation.[460] What was a crisis response (showing a QR code to enter a building) can morph into a permanent feature of civic life (a general-purpose digital wallet). If not carefully governed, this can extend emergency powers indefinitely, eroding civil liberties under the rationale of "better preparedness." Thus, crisis-born digital IDs can become Trojan horses for expanded state (or corporate) power.[461]

~

Beneath the sleek interfaces of digital identity apps and the cloud servers that store our data lies a very physical foundation: the minerals and materials that make modern electronics possible. This extractive base layer of digital technology connects our discussion

[459] Electronic Frontier Foundation, "COVID-19 and Digital Rights," 2021-2023 resource hub, https://www.eff.org/issues/covid-19

[460] World Health Organization, "European Commission and WHO Launch Landmark Digital Health Initiative to Strengthen Global Health Security," *WHO Newsroom*, 5 June 2023, https://www.who.int/news/item/05-06-2023-the-european-commission-and-who-launch-landmark-digital-health-initiative-to-strengthen-global-health-security.

[461] Jay Stanley. "Digital IDs Might Sound Like a Good Idea, But They Could Be a Privacy Nightmare." *ACLU*, 17 May 2021. https://www.aclu.org/news/privacy-technology/digital-ids-might-sound-like-a-good-idea-but-they-could-be-a-privacy-nightmare.

of sovereignty to environmental and postcolonial dimensions. States that are rich in minerals like lithium, cobalt, or rare earth elements find themselves at the crux of new power struggles, as these resources are essential for devices, data centres, and renewable energy tech. Just as identity has been financialised and instrumentalised into a commercialised product, so too have rare earth metals and mineral deposits[462] been assetised as critical fuel for the information economy. Both are presented as sovereign domains treated as extractive layers to be optimised and repackaged.

Rare earth elements (REEs) are a poignant example. These 17 minerals are used in components for smartphones, sensors, servers, and batteries – all building blocks of digital infrastructure. The global rush for rare earths and other critical minerals has been likened to a new "green rush," often playing out in the Global South. Countries like Madagascar have become hotspots for rare earth mining projects, touted as necessary for the green and digital transition to produce electric car motors, wind turbines, etc. However, local communities bear the brunt of environmental damage and social upheaval from these mining operations.

A 2025 report by the Debt Observatory in Globalisation (ODG) calls rare earth mining in Madagascar a case of "neocolonialism in the name of the green transition."[463] It argues that the drive by Global North countries for a low-carbon, high-tech future is offloading huge costs onto resource-rich but politically weaker states.[464] The report underscores that this adds to the "historical debt of the colonial and extractivist legacy" – meaning today's tech supply chains often perpetuate patterns of exploitation established in colonial times.[465] In plain terms, digital identity systems rely on smartphones ubiquity and are supported by always-on data centres in artificial climates, and all of these components are built on extracted cobalt from Congolese mines, lithium from Chilean salars, rare earths from Malagasy sands or Chinese hinterlands.

The environmental degradation (toxic waste, water depletion) and social dislocation (forced resettlement, labour abuses) that come with this extraction are often far removed from the end users in wealthy nations, creating an out-of-sight, out-of-mind effect. But

[462] Nicolas Niarchos, "The Dark Side of Congo's Cobalt Rush," *The New Yorker*, 31 May 2021, https://www.newyorker.com/magazine/2021/05/31/the-dark-side-of-congos-cobalt-rush.

[463] Observatori del Deute en la Globalització (ODG), *Neocolonialism in the Name of the Green Transition: Rare-Earths Mining in Madagascar* (Barcelona: ODG, 27 February 2025), https://odg.cat/wp-content/uploads/2025/02/NeocolonialismGreenTransition_ENG.pdf.

[464] Ibid.

[465] Nicolas Niarchos, "The Dark Side of Congo's Cobalt Rush," *The New Yorker*, 31 May 2021, https://www.newyorker.com/magazine/2021/05/31/the-dark-side-of-congos-cobalt-rush

they directly implicate questions of sovereignty and justice: who gets to profit from the digital boom,[466] and who gets poisoned?

Anthropologist Paul Gilbert notes that even mundane digital activities – like gaming – have material consequences for populations living atop these resources. Coltan price spikes, driven by consumer electronics and platforms like Sony's PlayStation, link the "seductive virtual world of Halo 3" with the violent extractive practices of militia-controlled mining in eastern Congo. In his words, "Citibank and other corporations… have negotiated directly with the ruthless occupants… who forced people to mine and plundered their villages."

> *‘[S]ites of mineral extraction, and the lives of those involved in mineral commodity situations, are implicated in broader systems of political economy. A great deal of attention is thus given to the manner in which artisanal miners in the Democratic Republic of the Congo (Smith 2011) or Madagascar (Walsh 2004) speculate over the cause of fluctuations in the world prices of the resources that they help transform into valued commodities. While seemingly the product of remote and opaque forces, these price fluctuations have profound implications for miners' capacities to build predictable economic futures for themselves. Hence for Jeffrey Mantz (2008, 41–42) an understanding of the coltan (or "digital mineral") trade demands a perspective that integrates "the seductive virtual world of Halo 3" (and the boom in coltan prices that resulted from the launch of Sony's PlayStation 2), as well as "Citibank and other corporations [who] have negotiated directly with the ruthless occupants of the eastern DRC… who forced people to mine and plundered their villages."’*[467]

This is the hidden substrate of digitisation, and by extension, digital identity; A world-spanning apparatus of enforced extraction, instability, and platform dependency. The infrastructure of clouds, chips, and networks powering digital identity is soaked in violence.[468] This extreme form of the entrepreneurship of the self, targeting specifically the people of the peripheries, is also accompanied with worsening health due to extreme polluting of the environment of the mining activities. Coincidentally, these tears in the social fabric of developing nations can be recycled, their destabilisation and ensuring crises presented as quasi-*Shock doctrine*[469] opportunities for administrative optimisation and

[466] Yann Philippin, "Gemalto est visé par une vaste enquête pour corruption en Afrique," *Mediapart*, 7 February 2023, https://www.mediapart.fr/journal/international/070223/gemalto-est-vise-par-une-vaste-enquete-pour-corruption-en-afrique.

[467] Kean Birch and Fabian Muniesa, eds., *Assetization: Turning Things into Assets in Technoscientific Capitalism* [Cambridge, MA: MIT Press, 2020], https://mitpress.mit.edu/9780262539173/assetization/.

[468] Roy Maconachie, "'We Miners Die a Lot': The Appalling Conditions and Poverty Wages of Congo Cobalt Miners," *Fast Company*, 4 February 2024, https://www.fastcompany.com/91021938/we-miners-die-a-lot-the-appalling-conditions-and-poverty-wages-of-congo-cobalt-miners.

[469] The *shock doctrine* is the theory that Neoliberal policymakers and corporate interests deliberately exploit

discipline delivered through digital identity.[470] [471] Digital identity thus becomes a post-facto rationalisation engine: rolled out to manage the very populations dislocated by the systems it legitimises.

~

The fraught political reality of the physical manifestations of digital identity were seen directly in our research. One participant highlighted the loss of sovereignty experienced by nations facing political turmoil or under outright attack, with their voting records held within the infrastructure of foreign allies or corporate stakeholders. This kind of complex scenario is the result of decisions not dissimilar from the crisis that saw Estonia fully digitise its identity system[472] yet regardless will almost certainly have unforeseen consequences down the line. A temporary restricted access "to e-services such as the health registry, banking or tax systems"[473] can sound like a minor drawback in the march for progress, but can be easily weaponised by state or corporate adversarial entities.

As some countries security forces have demonstrated recently with the tampering of hardware shipments in order to target opposition groups and civilian bystanders alike,[474] the novel threats arising from an ever intensified intertwining of the social and the technical cannot be easily discarded. Within the brittle digital society, the increased reliance on complex communication devices, and software as well as hardware stacks, out of reach of a given polity's legislative or civil spheres, can only hasten social and political dislocation.[475]

large-scale crises-wars, natural disasters, financial collapses-to impose rapid free-market reforms such as privatisation, deregulation and austerity while citizens are too traumatised to resist. Naomi Klein argues that this "disaster capitalism" uses the confusion and disorientation that follow a shock as political cover, converting public assets and social protections into new profit centres. In this view, radical economic change is less the product of democratic debate than of strategic manipulation of emergency, turning collective suffering into an engine for private accumulation; Naomi Klein, *The Shock Doctrine: The Rise of Disaster Capitalism* (London: Allen Lane, 2007), https://www.penguin.co.uk/books/414221/the-shock-doctrine-by-naomi-klein/9780141024530.

[470] Kerrie Holloway, Reem Al Masri and Afnan Abu Yahia, "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises," *ODI Global*, 6 October 2021, https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/.

[471] UNHCR, UNHCR Strategy on Digital Identity and Inclusion, February 2018, https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf.

[472] Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News*, 27 April 2017, https://www.bbc.co.uk/news/39655415.

[473] Kalev Aasmae, "Estonia's ID-Card Crisis: How E-State's Poster Child Got into and Out of Trouble," *ZDNet*, 13 November 2017, https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/.

[474] Maya Gebeily, James Pearson and David Gauthier-Villars, "How Israel's Bulky Pager Fooled Hezbollah," *Reuters* (graphics special report), 16 October 2024, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/.

[475] Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras, Sebastian Garcia and Veronica Valeros, "ENISA Threat Landscape for Supply Chain Attacks," *European Union Agency for Cybersecurity*, July 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

~

To analyse the evolving sovereignty landscape, thinkers have introduced terms like “kill switch sovereignty,” jurisdictional overflow, and “programmable personhood.” These frameworks help us understand how digital identity and infrastructure changes the power of states over citizens, and the power of external entities over states.

Kill Switch Sovereignty refers to the precarious situation where a state’s essential digital systems have an external “off switch.” Sovereignty traditionally implies autonomy where no outside power can simply turn off your government functions. But when critical platforms are foreign-run, that independence erodes. In 2023-2024, this occurred with Starlink in Ukraine, where a commercial provider could shut off a country’s internet in regions for alleged political gains, or the 2025 suspected disabling of Microsoft licences to key members of the International Court of Justice.[476] Although denied by Microsoft, the suspensions occurred around the same time as U.S. President Donald Trump handed down an Executive Order imposing sanctions on the ICC,[477] a sustained operation described as a ‘flagrant attack’ by media.[478]

The concept becomes starkly apparent when examining Russia’s experience following its February 2022 invasion of Ukraine. Within days of the invasion, Russian citizens discovered that their digital payment systems had effectively ceased functioning – a direct consequence of international sanctions targeting Russian financial institutions and payment processors. The most visible manifestation occurred on the Moscow Metro, where commuters faced widespread service disruptions as contactless payment systems that had become integral to daily urban life suddenly stopped working, leaving officials scrambling to respond to this paralysis.[479]

Russia’s predicament exemplifies how modern states, regardless of their geopolitical position, find themselves subject sovereignty by permission. The fact that Russian citizens’ ability to pay for public transport could be switched off by decisions made in distant

[476] Stefan Krempl, “Criminal Court: Microsoft’s email block a wake-up call for digital sovereignty,” *heise online*, 12 June 2025, https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html.

[477] Executive Office of the President of the United States, “Executive Order 14203 of 6 February 2025: Imposing Sanctions on the International Criminal Court,” *Federal Register* 90, no. 28, 12 February 2025, https://ofac.treasury.gov/media/933981/download.

[478] Guardian staff and agencies, “US Imposes Sanctions on International Court Officials in ‘Flagrant Attack’,” *The Guardian*, 20 August 2025, https://www.theguardian.com/us-news/2025/aug/20/trump-rubio-international-criminal-court-sanctions.

[479] Vixio, “Moscow Metro Pilots Homegrown Faster Payments, As Russia Eyes Payment Alliance,” Vixio Newsroom, 29 June 2022, https://www.vixio.com/insights/pc-moscow-metro-pilots-homegrown-faster-payments-russia-eyes-payment-alliance.

corporate boardrooms and foreign capitals underscores how digital infrastructure creates new vectors for external control over domestic affairs.

In 2019, when India abrogated Kashmir's autonomy, one of the first moves was literally a kill switch on the internet in that region. This amounts to nothing more than an example of a state asserting power over a territory by "turning off" connectivity.[480] The reversal is equally viable: a company or another country turning off services to assert power over a state. "Kill switch sovereignty" is essentially a warning that sovereignty by permission is not true sovereignty. With the global internet beginning to splinter off the back of deteriorating global political relations, some countries are pursuing national backup systems, such as Russia's sovereign internet RuNet project,[481] or China's BeiDou[482] satellite navigation system, to mitigate this risk.

Jurisdictional overflow examines how digital systems enable legal frameworks to transcend traditional territorial boundaries. When citizens utilize applications developed in foreign jurisdictions or store data internationally, the legal regimes governing those service providers extend extra-territoriality. The paradigmatic example involves U.S. law enforcement accessing foreign citizens' data stored by American companies, whereby U.S. constitutional protections and the CLOUD Act project beyond national borders into foreign citizens' digital lives.[483] U.S. tech platforms routinely target the individual accounts of citizens of countries including Crimea, Cuba, Iran, North Korea, and Syria, and point to state compliance as the reason: "*We're doing this because we have to.*"[484] This represents sovereignty restructuring, where corporations function as vectors for their home jurisdictions' legal reach. Conversely, the European Union's General Data Protection Regulation asserts global jurisdiction over any entity processing EU citizens' data, regardless of the processor's location, demonstrating reverse jurisdictional overflow.

For digital identity systems, jurisdictional overflow creates conditions where identity information operates under multiple concurrent legal regimes. Consider scenarios where

[480] Zach Rosson, Felicia Anthonio, Carolyn Tackett, Méabh Maguire, "Lives on Hold: Internet Shutdowns in 2024," *Access Now*, 23 February 2025, https://www.accessnow.org/internet-shutdowns-2024/

[481] Nadezhda Tsydenova, "Russia checks its internet can work if cut off from worldwide web," *Reuters*, 24 December 2019, https://www.reuters.com/article/technology/russia-checks-its-internet-can-work-if-cut-off-from-worldwide-web-idUSKBN1YS04J/.

[482] The State Council, "China to complete Beidou-3 satellite system in 2020," *Xinhua*, 27 December 2019, https://english.www.gov.cn/news/topnews/201912/27/content_WS5e05bd1bc6d03c1f1c161ce5.html.

[483] Stephen P. Mulligan, "Law Enforcement Access to Overseas Data Under the CLOUD Act," *Legal Sidebar, Congressional Research Service,* 2 May 2018, https://www.congress.gov/crs_external_products/LSB/PDF/LSB10125/LSB10125.2.pdf.

[484] Jon Porter, "GitHub Restricts Developer Accounts Based in Iran, Crimea, and Other Countries under US Sanctions," The Verge, 29 July 2019, https://www.theverge.com/2019/7/29/8934694/github-us-trade-sanctions-developers-restricted-crimea-cuba-iran-north-korea-syria.

Kenyan citizens' biometric data undergoes processing by French companies through contracts governed by UK law under British aid funding. Here, multiple jurisdictions become entangled within single identity systems;[485] These arrangements generate accountability gaps and legal recourse limitations, where citizens cannot effectively pursue remedies against foreign contractors, and governments lack oversight capabilities regarding vendor metadata usage. State sovereignty becomes conditional upon these overlapping jurisdictions, typically favouring powerful states where major technology companies maintain headquarters.

Programmable Personhood refers to the capacity for software systems to dynamically configure individual legal and social status. When identity systems operate digitally, rights and attributes become subject to modification through code execution or database updates. While this capability enables beneficial applications, such as Estonia's e-residency program granting foreign entrepreneurs digital business access. It also enables concerning implementations: China's evolving social credit system exemplifies algorithmic personhood programming, where behavioural assessments can dynamically restrict privileges including transportation access and financial services. Personhood becomes subject to algorithmic programming through behavioural monitoring and automated privilege adjustment.

Democratic societies demonstrate comparable elements through digital flagging systems that can instantaneously modify individual status that include sanctions lists, no-fly designations, or voting rights restrictions.[486] Such structures, especially when bound to a digital identity, fundamentally alter permissible activities. Pre-digital systems required bureaucratic and legal processes with inherent friction for such modifications. Contemporary digital systems enable instantaneous, often opaque changes implemented through code. Central bank digital currencies introduce additional dimensions: programmable money could theoretically restrict specific individuals' purchasing capabilities or implement expiration dates on currency holdings. While not inherently linked to identity systems, practical implementations would likely integrate with identification frameworks.

Within global power structures, programmable personhood extends to how dominant states or platforms can effectively determine individual status beyond their territorial boundaries. Platform decisions to ban accounts associated with particular groups can effectively exclude

[485] Kamau Muthoni, "Judge Quashes Parliament's Decision to Blacklist French Firm over 2017 Election," *The Standard*, 9 April 2020, https://www.standardmedia.co.ke/nairobi/article/2001367408.

[486] U.S. Department of the Treasury, Office of Foreign Assets Control, "*Specially Designated Nationals and Blocked Persons [SDN] List*," updated regularly,. https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

those individuals from global online discourse. Payment platform restrictions – exemplified by WikiLeaks' PayPal access termination[487] or the more recent pressure by Mastercard, VISA, Stripe and Paypal on video game sales platforms Steam[488] and Itch.io[489] and online creators to ban "sexual content," including LGBTQI themes – represent forms of programming economic participation eligibility. As digital identity wallets become essential for verification processes, access loss through state action, security breaches, or corporate errors could effectively exclude individuals from social participation, constituting digital de-personing.

Together, jurisdictional overflow, kill switch sovereignty, and programmable personhood demonstrate interconnected and inseparable dependencies. Kill switch scenarios often derive from jurisdictional overflow conditions, where enforcement mechanisms operate through the legal framework of the service provider's jurisdiction. Decisions to activate kill switches or modify individual status represent exercises in programming personhood. The attempted leverage of Ukraine's Starlink access during resource extraction negotiations represents perhaps the most concentrated example of all three issues operating together, demonstrating how these sovereignty challenges function simultaneously across multiple scales.[490] All three concepts are dramatically amplified when fused with digital identity systems.

~

From the European Union's pushback against U.S. cloud dominance to the Global South's navigation between opportunity and neocolonialism, every region is grappling with this dual-edged sword. As governments and corporations alike push digital identity ubiquity, states must reconceptualise sovereignty for the digital age. This means building resilience (so no external kill switch can paralyse the nation), asserting legal rights over data (to prevent unfavourable jurisdictional overflow), and safeguarding citizens such that their rights are not subject to an algorithmic whim. The EU's experiment will be an important bellwether – if a democratic bloc can create a trusted, sovereign digital identity framework that stands up to Big Tech, it could provide a model for others.

[487] John Hudson, "Why MasterCard, Visa and PayPal Are Wrong to Cut Off WikiLeaks," *The Atlantic,* 7 December 2010, https://www.theatlantic.com/politics/archive/2010/12/why-mastercard-visa-and-paypal-are-wrong-to-cut-off-wikileaks/343130/.

[488] Rick Lane, "Why Did Thousands of Adult Titles Just Disappear from the Biggest PC Gaming Marketplaces?" *The Guardian*, 29 July 2025, https://www.theguardian.com/games/2025/jul/29/why-did-adult-titles-disappear-from-steam-itch-pc-gaming-payment-processors.

[489] Ash Parrish, "The chaos and confusion of itch.io and Steam's abrupt adult game ban," *The Verge*, 29 July 2025, https://www.theverge.com/games/715299/itchio-games-delisting-payment-processor-paypal.

[490] Andrea Shalal and Joey Roulette, "U.S. Could Cut Ukraine's Access to Starlink Internet Services over Minerals, Say Sources," *Reuters,* 22 February 2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

If those efforts falter, we will see a continued drift toward a world where a handful of corporations and their home governments set the terms for everyone else's digital lives. ✳

10. Current and proposed identity solutions fail to prevent social engineering threats

> *"Stop! Right now, think of how many passwords and personal identification number (PIN) codes you have to remember. How often do you forget them? It is very inconvenient to remember those codes. Now, do you have your fingers, eyes, voice, and face with you? The answer hopefully is yes! Have you ever forgotten any of those body parts? Not very likely!"*[491]

> *"Slain man's thumb sliced off and used to steal from his mobile payment app, officials say"*[492]

Key Points

- Social engineering remains the primary vector for identity breaches; current digital identity systems consistently fail to address this.
- The fusion of presentation, authentication and authorisation amplifies vulnerabilities rather than mitigating them.
- Identity systems reduce complex persons into machine-readable fragments, creating abstractions that are easy to simulate, coerce, or weaponise.
- Efforts to "harden" identity via biometrics or protocols ignore the structural coercion of identity design and misdiagnose social risk as technical error.
- Attempts to reform digital identity through audits or encryption do not challenge its core flaw: its objectification and instrumentalisation of the self.
- The current paradigm treats identity as something to be verified, trading human context for machine certainty.
- As a result, these systems externalise risk, misplace responsibility, and entrench harm with increasing precision.

Despite the high-tech sophistication of modern digital identity solutions, for example multi-factor authentication and biometrics to blockchain credentials, such designs consistently fail to address the oldest and most pervasive threat: social engineering. **Our research shows that both current identity systems and many proposed and emergent solutions inadequately safeguard against social engineering, and in some cases create new vulnerabilities to it.** We argue that, at its core, the flaw of digital identity is a philosophical one, where the desire to automate certainty via *authentication* clashes with the incomplete or 'lossy' *presentation* of individuals and entities in a digital system.

This design carries a philosophical flaw that pairs with structural issues: identity is an appeal to authority, or are made up of rituals and bureaucracy that overwhelm those

[491] Paul Reid, Biometrics for Network Security (Upper Saddle River, NJ: Prentice Hall PTR, 2004), quoted in Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Durham, NC: Duke University Press, 2011), http://www.dukeupress.edu/when-biometrics-fail.

[492] Antonio Planas and Toby Lyles, "Slain Man's Thumb Sliced Off and Used to Steal from His Mobile Payment App, Officials Say," *NBC News*, 9 July 2024, https://www.nbcnews.com/news/us-news/slain-man-thumb-sliced-used-steal-mobile-payment-app-rcna161030.

unfamiliar with such a system. This uncertainty is capitalised on by an attacker, and as such, those most vulnerable in a digital identity system bear the brunt of social engineering attacks. **We argue that the historical underperformance and increasing complexity of the current paradigm of digital identity will never address the fundamentally social nature of identity attacks.**

~

Social engineering describes the manipulation of people rather than systems to gain unauthorised access, and the practice remains the leading cause of security breaches and identity-related fraud worldwide. Each year, cybersecurity reports highlight that human error or deception accounts for the majority of breaches. The Verizon 2023 Data Breach Investigations Report found that 74% of breaches involved the human element, with social engineering a significant contributor.[493] In the 2024 edition, researchers noted that 68% of breaches involved a non-malicious human element, such as phishing.[494] These figures show a persistent trend: attackers do not break systems, *they break people*.

For instance, in Sweden, the introduction of BankID saw an explosion in fraud via social engineering. According to Sweden's National Fraud Centre, criminals made about SEK 7.5 billion from fraud in 2023 via bank-impersonation (or "vishing"), where Callers pressure victims to log in and share bank e-ID or token codes. Vishing accounted for roughly SEK 708 million for the year.[495] The system's cryptography was not compromised; rather, trust was. Similarly, in the UK, as direct hacks became harder, scammers shifted tactics, exploiting victims into authorizing fraudulent bank transactions, costing over £500 million in 2022. This reflects a fundamental problem: technology-centric security often displaces rather than eliminates risk.

Digital identity systems merge various layers of presentation, authentication, and access to service into one seamless process. While this fusion increases efficiency, it also amplifies risk. Philosopher Grégoire Chamayou describes this as a hardcoded feature of digital identity, "*a particular type of innovation platform, where functions of identification, authentication and authorisation are tied together.*"[496]

[493] Verizon, *2023 Data Breach Investigations Report*, 2023, https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf.

[494] Verizon, *2024 Data Breach Investigations Report*, 2024, https://www.verizon.com/business/resources/T17c/reports/2024-dbir-data-breach-investigations-report.pdf.

[495] Nationellt bedrägericentrum Polismyndigheten, *Brottsvinsterna för bedrägeribrottsligheten 2023*, 15 April 2024, https://polisen.se/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottsligheten-2023.pdf

[496] Grégoire Chamayou, *A Theory of the Drone*, trans. Janet Lloyd (London: Verso, 1 May 2015).

In *Digital identity as platform-mediated surveillance,* Sylvia Masiero and Viktor Arvidsson goes further:

> *"A core-complements architecture is effectively capable of matching individuals not just with their entitlements, but with their records in state and international databases, whose presence deters vulnerable groups from enrolling into schemes for accessing core services. Portrayed by Mukhopadhyay et al. (2019) as a way to improve the distribution of benefits through scaling,* ***the architecture of digital identity platforms effectively enables interoperability among systems****: Masiero and Arvidsson (2021) note that such an architecture produces unjust exclusions, making access to services conditional to biometric user authentication."*[497]

One outcome of the intent of the design of identity frameworks is a kind of 'interoperability' with each other. Cybernetics, the study of systems and their self-regulating mechanisms, plays a crucial role in shaping modern digital identity. In cybernetic models of information and communication, systems are designed to process, transmit, and integrate data as efficiently as possible. This approach assumes that identity can be fully captured and represented through digital records, which then communicate seamlessly with other systems. Traditional identity systems, such as paper-based registries, deliberately introduced friction to limit information sharing and maintain privacy. Digital identity, by contrast, thrives on interconnectivity, making information exchange instantaneous and automatic.

Chamayou describes this as an effort to combine all aspects of a person's digital footprint into one unified record where the aim of the system's design is to *"to fuse together [...] different layers of information and pin them all together so as to combine in a single item all the informational facets of one particular event [...]."*[498]

In both policing and surveillance, as well as in social engineering attacks, the process of assembling an individual's identity follows the same fundamental logic: aggregating scattered fragments of personal data to construct a version of the person that can be acted upon. Journalist Jacob Ward, in *The Loop*, highlights how law enforcement institutionalises this principle through *"fusion centres,"* which link federal, state, and local agencies, enabling them to rapidly share identity data, including facial recognition matches, with organisations like the FBI.[499] This system is meant to enhance security and efficiency;

[497] Silvia Masiero and Viktor Arvidsson, "Degenerative Outcomes of Digital Identity Platforms for Development," *Information Systems Journal* 31, no. 6, November 2021, https://doi.org/10.1111/isj.12351.

[498] Grégoire Chamayou, *A Theory of the Drone*, trans. Janet Lloyd (London: Verso, 1 May 2015).

[499] Ibid.

it also mirrors the methods used by social engineering adversaries who weaponize identity for exploitation.[500]

At its core, both law enforcement surveillance and social engineering operate by crafting a persuasive and actionable digital representation of a person that is nothing more than a digital diorama. Whether it is an intelligence officer linking phone records to credit history, and travel logs or a scammer using leaked credentials from public records to mimic a loved one, the end goal is the same: to make the digital identity real enough that institutions or individuals respond to it. In this way, the identity frameworks that underpin policing are structurally identical to those that facilitate fraud.

This is the outcome of identity: When law enforcement centralises and interconnects identity data, it does not merely enhance institutional power – it reinforces the fundamental coercive nature of digital identity itself. The same markers that allow authorities to track and categorise individuals also serve as tools for manipulation, whether in the hands of the state, a scammer, or an employer assessing a social credit score. The core mechanism is identical: through the sum of its parts, identity is always something that is wielded against the individual, never something they truly own.

~

While separating and differentiating each layer of digital identity is often seen as a safeguard, this very separation can introduce new risks, as these layers are fundamentally enmeshed. In civil society and policy discussions, there is a tendency to isolate the user-facing aspect of digital identity from the broader infrastructure that underpins it. This perspective suggests that if harm arises from how identity is presented or authenticated (especially in cases involving biometrics), then auditing the infrastructure and refining protocols will address the issue.

However, this approach misdiagnoses the problem. The harm is not simply a function of flawed implementation; It is embedded in the very architecture of digital identity itself and attempting to solve surface-level issues without addressing the coercive structure that digital identity operates within only perpetuates its vulnerabilities, making it easier to rationalise the expansion of these systems rather than questioning their necessity.

In research interviews, we found that participants constantly struggled to verbalise ways in which the radical defences required could be achieved:

[500] Grégoire Chamayou, *A Theory of the Drone*, trans. Janet Lloyd (London: Verso, 1 May 2015)

"A lot of that has less to do with the voter identity part and more about ballot marking, counting, transmission. There's all sorts of uses of technology like when you use a ballot marking device for example, and then the ballot marking device has an electronic workflow to a results transmission system.

And so from being able to observe a ballot going through, like a ballot being marked by a human and being put in a box, to this ballot being electronically marked [to verify its existence]. So there's an obfuscation of what's going on and that builds an inherent amount of distrust [...].

It is an inevitable part of the march of modernity forward that technology is going to get introduced into the process of voting, so my view of it is, given that inevitability, it is my job and the job of civil society to enable that in the safest manner possible. The safest manner possible is almost always, in my view, one of an incremental approach that is validated and tested on a small scale and then in successive larger scales until it can be scaled to the national level for a national-level election."

Research participant
International elections observer

While well-intentioned, this structuralist approach reveals an appalling reality: **digital identity is being woven into democratic processes even as we collectively acknowledge its profound flaws.** The insertion of identity-driven technologies into voting systems, governance, and civil society is not an outcome of careful deliberation, but of an unrelenting, almost resigned march forward, a kind of linear perception of technological progress that few feel empowered to resist. What is most alarming is that the people tasked with safeguarding these systems – from their original designers to the auditors retroactively attempting to correct course – often recognise the dangers yet remain trapped in a framework that assumes technological expansion must continue, no matter the cost.

When asked to describe the threats of digital identity, participants overwhelmingly treated sometimes shocking risks as obstacles to be incrementally refined rather than fundamental issues to be reckoned with. The assumption that identity systems can be continually patched and reformed, rather than confronted at the root, allows their expansion to proceed unchecked. Such a position justifies further entrenchment under the guise of control, security, efficiency, user self-sovereignty and modernisation, all while exacerbating the very vulnerabilities it purports to solve.

When parsed against existing literature – everything from the marketing materials of cybersecurity firms promising seamless protection to policy documents from the EU outlining "trust frameworks" and "resilience strategies"– the gap between what is said to be happening and what is *actually happening* with digital identity is so wide, it is almost like being gaslit. The structuralist tinkerer, forever adjusting the mechanisms of authentication and verification, is pitted against an existential threat that actively tears at the social fabric. The language of reform disguises the reality that these systems are not merely flawed, but inherently coercive, reinforcing hierarchies of control while exposing individuals to new forms of manipulation and exploitation. The overwhelming response to these dangers – more audits, better protocols, tighter encryption – feels less like a genuine attempt at security and more like an effort to reassure the public that the system is salvageable when, in reality, the very premise of digital identity remains deeply unstable.

~

The two approaches – fusionist and structuralist – both miss the main issues plaguing digital identity. Data, at its foundation, is an objectifying force. It does not recognise context, nuance, or the fluidity of human existence. Instead, it flattens, categorizes, and reduces individuals into discrete, actionable units. As such becomes a tool to be wielded by social-engineering attackers. A piece of technology is not born as an unfettered good whose shortcomings can be patched and improved, but is often thoroughly biased, immensely destructive, and very quickly subject to degeneration.[501] Moreover, "a digital platform may well be successfully implemented yet negatively affect the target system in which it is incorporated."[502]

Digital identity, then, is evidently more than just an authentication mechanism: It is an enforced reconstitution of the self through a bureaucratic and technical lens, transforming a complex, relational being into a dataset that can be acted upon. This reductionist process is why digital identity is so uniquely vulnerable to social engineering: it turns the person into an abstraction, a collection of verifiable markers that can be convincingly simulated, stolen, or weaponised. When identity becomes a standardised artifact rather than an emergent social phenomenon, it ceases to function as a representation of the person and instead becomes a mechanism of control over them.

[501] Silvia Masiero and Viktor Arvidsson, "Degenerative Outcomes of Digital Identity Platforms for Development," *Information Systems Journal* 31, no. 6 [November 2021]: 903-928, https://doi.org/10.1111/isj.12351.

[502] Ibid.

To understand digital identity in its entirety, from authenticating into a Google Drive, to being scammed, to doxxing, to automated creditworthiness decisions, is to understand that it is fundamentally built on coercion. It is a system of markers that demands acceptance by presenting itself as the only means of access, the only way to prove one's legitimacy, while simultaneously exposing individuals to the risk of manipulation. Through the aspiration of the fusionist, identity's most base promise – *"I authenticate, therefore I am"* – is an appeal not to truth but to the belief of another, a belief that is often unwarranted.

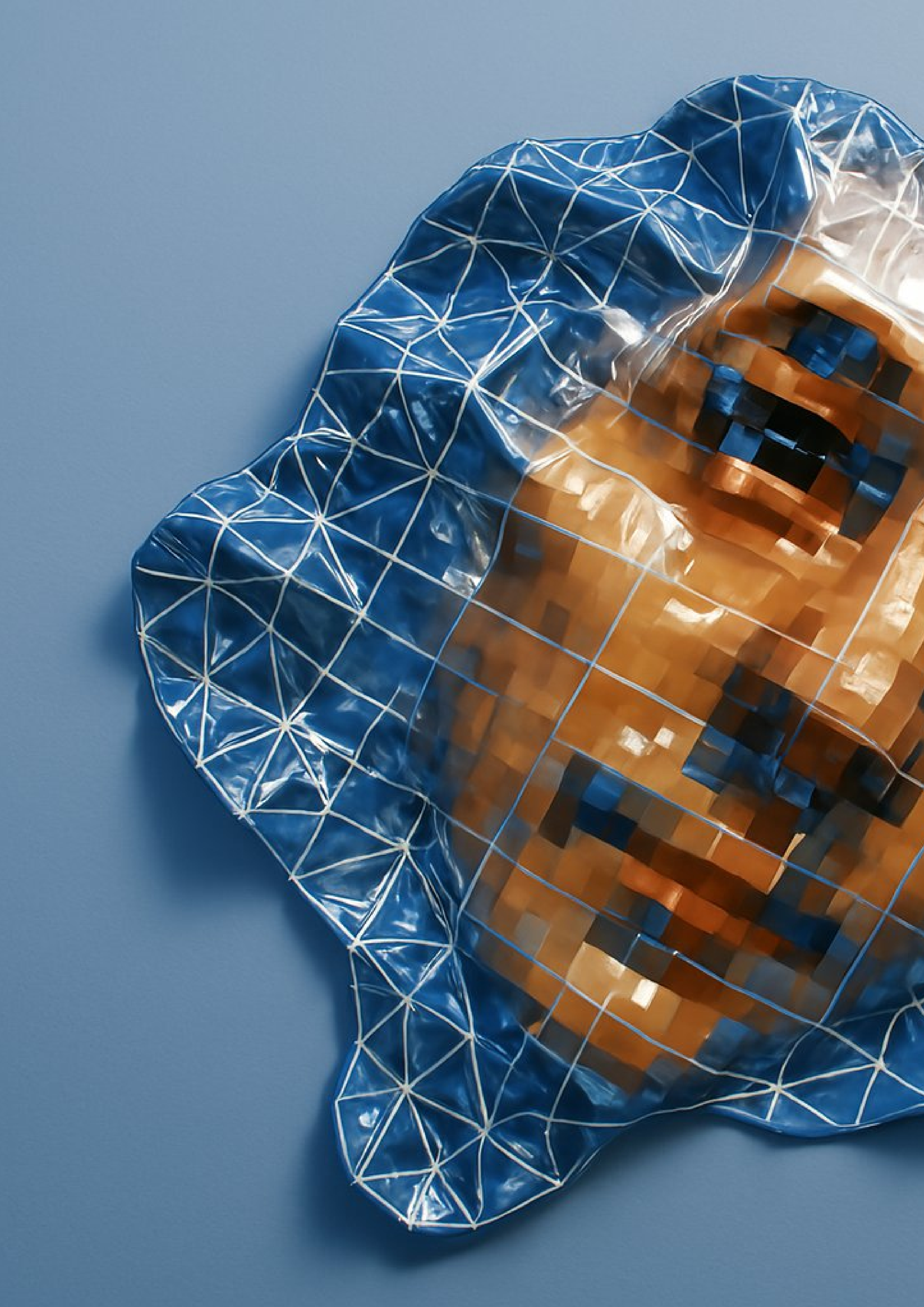
This is why digital identity systems, no matter how well-implemented, remain inherently coercive. They require an individual to prove themselves according to predefined, machine-readable parameters that often fail to capture the full scope of human experience. This structure is is intentional – through the desire to reorganise the world into efficient systems, digital identity is a by-product of a world organised for management disguised as individual empowerment. As such, digital identity prioritises technical verification over relational trust, and becomes remarkably easy to exploit. A fraudster does not need to impersonate a person in their full complexity; they only need to convince a system that they meet its narrowly defined criteria for authentication.

~

Today, identity-related social engineering leads to financial ruin, loss of services, emotional trauma, and even national security issues. This damage is so widespread, so systemic, that it has almost become invisible – treated as an inevitable outcome of modern identity systems rather than a fundamental design flaw. Our current approach favours incremental technological solutionism over social resilience, embedding coercion into every layer of digital identity. Regardless of their innovations, all current digital identity systems prioritise verification over trust, security over autonomy, and efficiency over humanity. Through the promise of sovereignty, they externalise risk, shifting the burden of security onto individuals while absolving the system itself of responsibility. A well-designed and encrypted digital identity framework will always be vulnerable to those who attack it from outside the system, from the spaces that Cybernetics discards as entropy.

In the face of these losses, financial devastation, systemic exclusion, and the erosion of personal autonomy, what remains most alarming is the level of inaction and the enduring faith in a broken model. Rather than confronting the fundamental flaws of digital identity, institutions and policymakers continue to tinker at the margins, reinforcing a system that has already demonstrated its incapacity to protect the people it claims to serve.

Secure identity should be understood as a social performance, and the current implementations – which treat it as a credential – must be treated with utmost suspicion across all aspects of the digital identity design and policy ecosystem. The victim of digital identity, whether via fraud, identity theft, or repression, must be considered for what they are: individuals and communitys grappling with a designed system that operates with absolute power asymmetry. Until suitable alternatives emerge that can truly whether the threats identified in this report and beyond, the systems that claim to protect us will continue to harm entire societies with greater and greater precision. A system built to recognise identity, backed by immense opportunity for wealth, influence or control, will always invite those who can best impersonate it. ✳



Recommendations

Against the backdrop of a particularly set of key findings and conclusions on the landscape of digital identity, we sought to explore progressive and optimistic interventions to the multitude of immediate and future crises that form the digital identity event horizon. The following recommendations are consequently not future-oriented policy speculations; they are immediate interventions. Each recommendation emerges from a world already destabilised – where identity infrastructures have failed in crisis, where sovereignty is conditional, and where digital identity is weaponised as often as it is celebrated. While existing discourse around digital identity is dominated by promises of inclusion, access, and innovation, our research makes it clear that the urgent threats of digital identity are multi-faceted and demand strategic intervention.

In observing and interacting with the collaborators of this research, the research participants and the wider community in which we operate, this chapter leverages the broad range of expertise to produce a myriad of immediately-implementable action: Some recommendations target the technical architecture of identity systems, others aim at legislation, platform governance, or user experience. These interventions span law, software design, platform governance, and crisis response. They reflect the layered, cross-domain nature of digital identity infrastructure. Accordingly, each recommendation is aimed at actors across domains: policymakers, engineers, advocates, and those tasked with building or resisting these systems.

We do not outline a perfect system. Instead, we set minimum thresholds for harm reduction, reversibility, and agency. These recommendations are ultimately to prevent the brittle nature of the current and future digitised society.

Define digital identity clearly, beyond state and market needs

Digital identity remains undefined in most legal and infrastructural regimes, its contours shaped not by consensus, but by vendor convenience, state opportunism, and inherited user experience patterns. This lack of definition generates structural ambiguity that erodes accountability across platforms, institutions, and legal systems. It also enables coercive defaults: identity systems that centralise power, undermine user agency, and collapse human complexity into surveillance primitives.

We recommend that states, consortia, and standards-setting bodies formally define digital identity as a negotiated systems framework that includes specific exclusions and required inclusions. This definition must be structured to:

1. Close accountability gaps in digital identity infrastructure (including spheres of identity and their associated harms);
2. Prevent market-led enclosure of identity schemes by cloud platforms, vendors, and token-based governance models;
3. Enable situated definitions, where local actors, states, cultural groups, and regions, can construct their own compatible identity logic within a defined systems frame, and;
4. De-centre digital identity as the singular mode of legal personhood.

This requires consensus on baseline exclusions:

- Digital identity cannot be defined by or dependent on biometric recognition, even as a user experience shortcut;
- Digital identity cannot be immutable;
- Identity systems must separate authentication from presentation;
- Centralised account ownership, tokenised identity, persistent behavioural profiling, and blockchain permanence are incompatible with safe, adaptable identity frameworks, and;
- There is no such thing as a decentralised identity if modification and governance are controlled by vendors or require system-level literacy beyond that of the individual user.

And baseline inclusions:

- Every digital identity must have a non-digital or analogue companion to ensure access under disruption or exclusion;
- Identities must be revocable, mutable, and interruptible without retaliation or systemic degradation;

- Custodianship and power of attorney must be embedded into the definition – people must be able to assign, reclaim, or transfer identity governance with granularity;
- Individuals must be able to maintain multiple identities that are not forcibly linked, and these identities must respect context and scoping, and;
- Systems must support interruption-resilient operation, including fully offline modes.

This recommendation does not aim to produce a universalised global identity model. On the contrary, it asserts the right of many identity definitions, including state, local, institutional, or regional, to coexist within a systems frame that preserves individual agency, coercion resistance, and mutability. It is not the role of any one actor, state, platform, blockchain, or vendor, to define the self for others. **Instead, the goal is to build a definitional floor beneath which no identity system can fall.**

This floor requires consensus, sensitive to context and not not on a singular implementation, but on a common refusal to permit exploitative, brittle, or coercive systems to define what counts as identity. **Without shared parameters or collective agreement on what digital identity is and is not, we will continue to legislate and engineer systems with mismatched assumptions, incompatible goals, and unresolvable harms.** Every failed integration, every privacy breach, every unaccountable platform exploit stems from this absence.

Consensus here is a recalibration of responsibility. Policymakers, technologists, and civil infrastructure builders must shift from imagining identity as a solved technical paradigm to recognising it as an ongoing negotiation between power, personhood, and system design. This requires courage: to say what identity must never be, to insist on rights of refusal, and to design from a place of pluralism rather than control.

There can be no safe digital infrastructure without first agreeing on who a person is allowed to be within it. ✳

Resist immutability as a governance default

Immutability is a design choice with significant consequences, framed as a neutral and inevitable part of a dataset's stability. In digital identity systems, immutability transforms the subtle changes of a person, their ephemeral physical states, their relationships, and performative selves into permanent artefacts that escape the control of those they claim to represent. When systems default to storing identity attributes as fixed records assembled from unchangeable names, gender markers, biometric hashes, unique identifiers, they reproduce the worst logics of colonial governance, making the self legible to power but illegible to itself.

We recommend that policymakers and public sector technologists *reject immutability as a governance default* in digital identity infrastructure. Instead, digital identity systems must embed revocation, expiry, mutability, and contextual deletion as foundational design capabilities as baseline features of legitimate identity governance.

Irreversible identity architectures already harm millions, and this is reflected throughout the findings: trans identities are erased by immutable record systems, FaceID biometric training is poisoned by everyday UX interactions,s inaccurate records persist across border and welfare systems, commercial DNA databases collapse under financial pressure while holding genomic markers that outlive consent. Immutability enables surveillance, erodes dignity, and denies people the right to outgrow or reclaim themselves.

While some records must be preserved for legal or civic purposes, this must never justify universal immutability. History teaches us that 'immutable' records have always disproportionately harmed the most vulnerable: marginalised populations, colonised communities, political opponents, and those navigating borders or systemic violence. Systems that cannot forget become instruments of persecution. Instead, identity systems must be built on:

- **Expiry**, via time-bounded attributes and proofs, with lifespans determined by context and user consent;
- **Revocation**, via the ability to retract identity assertions by the subject, by authorised custodians, or by automated conditions;
- **Mutability**, via the capacity to update, correct, or evolve identity markers, including name, gender, affiliations, and metadata, without creating duplicate selves, and;
- **Deletion,** via full, user-invocable erasure of data, relationships, or identifiers that are no longer valid or desired.

Governments and institutions must reframe identity as a dynamic negotiation that is structured enough to function, but fluid enough to reflect reality. Critics will claim that refusing immutability is a rejection of integrity or accountability, but such rigour is meaningless at the cost of systemic harm. Instead, the refusal of immutability is to accept that people should live their lives within systems that deny their right to change, to escape, or to heal.

Governance built on permanent identity will always eventually fail the populations it claims to serve. Resilience begins when systems learn to let go. Immutability may appear to offer certainty, but in a world where the ground shifts beneath us, it becomes an intolerable vulnerability. It fossilises identity into a system that cannot adapt to violence, cannot absorb political rupture, and cannot accommodate repair. Forcing people to persist within outdated or adversarial records ensures that systems will not only fail to protect them, they will become complicit in their targeting. A trans person caught in an outdated registry. An exile identified by facial scan. A political dissident unable to revoke old affiliations. A single parent suppressed by their precarity. These are not edge cases. They are inevitable outcomes of design choices made without the right to disappear. Infrastructures that cannot be revised will break under the weight of the future. Worse, they will take people with them.

Resilient systems do not always cling to permanence. They encode the capacity for forgetting, transformation, and withdrawal as civic rights. **Letting go is good governance.** ✳

Separate authentication from presentation

The conflation of authentication and presentation is one of the most enduring and corrosive errors in the design of digital identity systems. When a system treats *how you prove you are you as equivalent to what others see of you*, it creates an unresolvable tension between trust and exposure, one that adversaries have exploited since the birth of the internet.

We recommend a strict conceptual and architectural separation between authentication (proof of access or legitimacy) and presentation (what identifying attributes are revealed, to whom, and under what terms). This separation must be enforced at both protocol and implementation levels as a foundational governance constraint.

As we detail in the key findings, current digital identity systems collapse these layers by default. Such tight coupling creates easily defeated and brittle systems of trust: ones where impersonation, phishing, and misattribution are inevitable modes of failure that allow non-technical adversaries to defeat sophisticated digital security defences.

Whether through spoofed email headers or voice synthesis, adversaries exploit the same core flaw: the assumption that authentication is identity, and that identity must be shown to establish trust. This model – Cartesian in its faith, colonial in its reach – has governed **three decades of digital security, and failed catastrophically throughout.**

We cannot defend users from deepfakes, platform impersonation, or spear phishing if our systems continue to broadcast identity in every handshake. Therefore the only conclusion we can reach is that presentation is not a proof. To compensate, technologists and systems designers should begin to consider identity presentation as a performance to be negotiated in context. In this context, authentication must become silent and separated. Presentation must become conditional and mediated. The two layers of digital identity must be as distinct as encryption and metadata.

The beginnings of a better model already exist: relationship-scoped identity keys, context-specific pet-names, systems where people are known as someone to someone, rather than globally. But until our infrastructure encodes this separation as default, even the strongest cryptography will be betrayed by the false promise of recognisability.

Digital identity systems must stop asking users to perform their identities every time they prove access. We must build systems that do not conflate being trusted with being known. Until then, every authentication is an invitation to be tricked. The tools of social engineering – phishing, impersonation, manipulation of trust signals – remains the most effective and devastating class of digital attack. It is responsible for the majority of successful intrusions, espionage operations, and credential breaches across both public and private sectors. The economic damage is measured in billions annually. No technical patch, no biometric scan, no multi-factor token, no password manager, has come close to solving this, because the core vulnerability is architectural.

As such, no current or emergent digital identity framework can meaningfully resist this category of attack until it severs the representational self from the act of authentication. The way out is to embark in a comprehensive rethinking of what it means to be known in a system, and what kind of knowledge an adversary can exploit. If authentication is about access, and presentation is about relationship, then systems must learn to keep the two apart. **Anything less is a weaponised trust ceremony waiting to be abused.** ✳

Develop forward-thinking legislation for digital identity

As identity systems are deployed at scale across platforms, borders, and legal regimes, the absence of legislation to account for their abuse enables discrimination, fraud, and violence to flourish without consequence.

We recommend the development of legislative frameworks that recognise digital identity as both an administrative tool and a system that can cause harm, enable discrimination, and contribute to real-world violence. Lawmakers must treat digital identity as a civic domain governed by rights, subject to abuse, and in need of both protection and repair.

When digital identity is manipulated, coerced, falsified, or exposed, it is still too often treated as a technical fault or user misunderstanding. For example, across Europe, the response is codified by procedural half-measures like the Right to Object and the Right to Forget, which attempt to negotiate between the injured and the aggressor rather than confronting the structural design failure at the heart of the harm. This form of mediation dignifies exploitation as a misunderstanding and delays accountability. Instead, these violations must be recognised as social injuries.

We call for the abuse of digital identity to be treated as an aggravating factor in the sentencing of crimes across four key domains: corporate misconduct, financial fraud, systemic discrimination, and violent or targeted criminal acts. The precedent already exists: hate crimes carry aggravated sentencing because the identity of the victim is part of the motive. We argue that identity manipulation, regardless of intent to deceive, control, or harm, should be treated with the same gravity as any crime that tears at the fabric of society itself. A man who catfishes a woman on a dating platform and commits violence has not simply lied, he has exploited a digital trust system, weaponised representation, and performed harm through the architecture of identity itself.

Digital identity systems have long been shaped by their capacity to categorise and control. Trans individuals forced to navigate mismatched records. Indigenous populations are excluded from government services. Diaspora communities are penalised by inflexible credentialing. From the corporate world, If a company uses digital identity data to exclude access, enforce discrimination, or entrench inequality, that is not non-compliance. It is structural harm. If a platform enables identity laundering in financial crime, the breach should be considered as institutional complicity. If a perpetrator falsifies a digital identity to gain trust, lure a victim, or target someone for violence, the digital identity itself becomes a weapon. The law must acknowledge this.

To legislate with foresight is to name these systems as vulnerable, and their misuse as socially corrosive. We must enshrine not only protections, but meaningful avenues for redress including legal recognition that digital identity misuse harms individuals, distorts relationships, and threatens trust at a fundamental level.

Abuse of digital identity is an attack on the scaffolding of trust that modern life depends on. The law must rise to meet it. We urge legislators, regulators, and legal practitioners to treat digital identity as a critical civic infrastructure capable of being misused for personal gain, political suppression, and social control. **To do otherwise is to abandon the very populations these systems claim to serve.** ✳

Implement digital death, transfer, and guardianship protocols in digital identity systems

Current digital identity systems do not adequately account for incapacitation, death, or loss of access. This gap places survivors, dependents, and legal representatives in difficult and often harmful positions, particularly in healthcare, financial services, and digital platforms. As digital identity becomes increasingly integrated into essential infrastructure, it is necessary to ensure that systems can support estate administration, guardianship, and delegated authority in a consistent and reliable way.

We recommend that digital identity systems integrate protocols for death, incapacitation, and loss of access, ensuring that survivors, dependents, and legal representatives can act without barriers or undue hardship. These protocols should be explicitly designed for three critical areas: estate administration following death, guardianship for children or those with disabilities, and the delegation of power of attorney.

As digital platforms, particularly tech companies, increasingly offer “family” or “trusted contact” options, the historical failures in these systems are glaring. The defaults are often inadequate, coercive, or inaccessible to those who need them most. Too many platforms leave families scrambling to recover access after the death of a user, while others fail to grant guardians the rights to manage accounts or health data for incapacitated individuals. In many cases, these systems entrench vulnerabilities, leaving dependents or survivors with limited options, even when they have clear, legal standing.

In making this recommendation, we acknowledge that, to some degree, custodianship protocols may justify the creation of access mechanisms for trusted parties. However, it is critical to emphasise that this does not advocate for backdoors in public key cryptography or undermine fundamental security. **Systems that allow trusted custodianship must be designed in a way that preserves the integrity of cryptographic systems and the privacy of users, without compromising the principles of trust, transparency, and security.** The moment cryptographic backdoors are introduced, custodianship becomes impossible to guarantee, and these systems will fail to serve their intended purpose.

The inclusion of these protocols is not just a technical necessity but a moral imperative. Digital identity is already a critical part of how people access health care, manage finances, and maintain relationships with their families. Without protocols for digital death, guardianship, and temporary delegations, we leave society's most vulnerable members exposed to systems that offer no recourse or repair. Digital identity infrastructure must account for the full lifecycle of access and control. **The human world of advocacy must not be erased by the limitations of cryptography.** ✳

Prioritise threat modelling in digital identity rollouts

Digital identity systems are increasingly deployed across critical infrastructure, yet many are designed and implemented without systematic threat modelling. This leaves systems vulnerable to coercion, exploitation, and failure when used in complex social, legal, and political environments. Without structured modelling of adversarial behaviour and sociotechnical risks, identity systems will continue to reproduce harm at scale.

We recommend that all digital identity initiatives, whether implemented by states, corporate actors, or public-private partnerships, include formal threat modelling as a non-optional requirement at the outset of system design. This modelling must go beyond technical risks and account for coercion, targeted surveillance, state and non-state adversaries, exclusion, and misuse by platforms, employers, and political entities. It should include threat actors across levels of power, from individuals conducting fraud to governments misusing identity systems for control or repression.

Baseline requirements for threat modelling should be clearly defined and independently auditable. These should include:

- Modelling of coercive scenarios (e.g. domestic violence, state overreach, employer abuse);

- Analysis of cross-jurisdictional risk (e.g. political persecution, data sharing regimes);

- Evaluation of exclusion risks under infrastructural failure (e.g. outages, loss of device access, migration);
- Consideration of identity correlation, linkability, and the collapse of pseudonymous or relational identities, and;
- Review of consent boundaries under duress or asymmetrical power relations.

This threat modelling artefact should be treated as a core part of public procurement and regulatory compliance. It must be reviewed at major development milestones, verified through third-party audit, and available for legal discovery in cases of harm. Where systems serve vulnerable populations, affected groups should be consulted directly in the modelling process. Identity systems that fail to produce or update these models should be considered incomplete and unsuitable for deployment.

Treating identity infrastructure as neutral or benign during rollout phases creates systemic risk and undermines trust. Incorporating structured, mandatory threat modelling is essential to ensure these systems can withstand misuse, protect users, and remain adaptable to evolving political and technological conditions. ✳

Close loopholes in financial legislation that shield institutions behind biometric identity

In jurisdictions across the world, financial institutions continue to rely on biometric and biometric-adjacent authentication systems, such as facial recognition, fingerprint scans, and behavioural profiling, to shift liability away from themselves and onto the user. These systems are routinely treated as evidence of informed consent or authorisation. When fraud occurs, institutions cite biometric interaction as proof that “reasonable steps” were taken, and reject restitution claims on that basis. This practice is widespread, persistent, and incompatible with meaningful consumer protection.

We recommend immediate legal reform to close these loopholes by eliminating the treatment of biometric authentication as sufficient evidence of user consent. All biometric systems are probabilistic, irreversible, and increasingly subject to coercion, spoofing, and simulation. They must not be considered definitive proof of authorisation in cases of fraud or identity misuse.

This principle of consumer financial protection is not new. In the United States, the *Electronic Fund Transfer Act of 1978*, which formalised a consumer’s right to dispute unauthorised electronic transactions, governs modern cases. But its legal and ethical foundation goes back further; Case law and commercial codes from the early 20th century made clear that banks must make customers whole in the event of unauthorised transactions, unless the customer was demonstrably negligent.

While the U.S. codified this principle early through case law and later through Regulation E and the UCC, many other jurisdictions adopted similar doctrines, either through common law inheritance or consumer protection frameworks as digital finance evolved:

- In the United Kingdom, under common law principles and the Payment Services Regulations 2017 (which implement the EU's PSD2), a bank must refund unauthorised payments unless the user is proven to have acted fraudulently or with gross negligence;
- In the European Union, Article 74 of PSD2 (Directive (EU) 2015/2366) requires payment service providers to refund unauthorised transactions unless they can prove the payer acted fraudulently or failed to protect personalised security credentials. This sets a strong default in favour of the user, which has been inconsistently enforced, especially when biometrics enter the picture;
- In Australia, The ePayments Code, administered by ASIC, provides similar protections. It requires institutions to reimburse unauthorised transactions unless the user contributed through fraud or a significant failure to protect access. However, ambiguity around what constitutes "reasonable steps" often creates a loophole for biometric systems;
- In Canada and New Zealand, protections are derived from English common law, with case law affirming that banks bear responsibility for unauthorised withdrawals unless they can prove user fault. Consumer protection statutes support this view but have not been consistently adapted to cover biometric authentication;
- In India, under the Reserve Bank of India's (RBI) guidelines on electronic transactions (2017), banks are required to credit unauthorised transaction losses back to customers if the fault lies with the bank or system provider. If the customer reports fraud within a reasonable time-frame, they are entitled to zero or limited liability. However, this protection becomes weaker when Aadhaar-based biometric authentication is involved, where fraud claims are often dismissed due to system trust;

- In Singapore, the E-Payments User Protection Guidelines issued by the Monetary Authority of Singapore (MAS) establish that users should not be held liable for unauthorised transactions unless they were grossly negligent or failed to report the fraud promptly. Biometrics are included under "access credentials," but there is growing concern that institutions use biometric logs as conclusive proof of user action, mirroring problems seen elsewhere;
- In South Africa: The Financial Sector Conduct Authority (FSCA) enforces principles of "fair treatment" and requires financial institutions to investigate unauthorised transactions. South African courts have ruled that institutions cannot rely solely on system logs to deny claims. However, there's limited regulatory language explicitly addressing biometric systems, leaving a potential gap;
- In the United Arab Emirates, the Central Bank of the UAE's Consumer Protection Regulation (2021) establishes liability limits for consumers in cases of fraud. However, similar to other jurisdictions, the implementation of biometric and facial recognition in fintech and digital ID schemes is largely unregulated in this context, allowing banks to cite biometric "proof" as justification to avoid redress, and;
- In Brazil, under the Banco Central do Brasil regulations on unauthorised payments and the Consumer Defence Code (Código de Defesa do Consumidor), banks are liable unless they can clearly prove that the user acted with intent or negligence. Courts have ruled in favour of consumers in many cases involving phishing or fraud, even when biometric authentication was used.

That duty of care widely adopted internationally has been steadily eroded by technical systems that shift risk onto users without providing meaningful recourse. As a result, all of these frameworks must be amended to shift the burden of proof onto institutions. Biometric interaction cannot be treated as definitive authorisation without broader evidentiary support. Financial service providers must demonstrate, using multifactorial and independently auditable evidence, that consent was not only technically registered, but contextually informed, without coercion, and intentional. **Biometric authentication must be downgraded to a single signal among many, it is not a secure authentication strategy.**

This recommendation extends beyond conventional biometrics to include biometric-adjacent identity systems: behavioural fraud detection, device fingerprinting, passive location-based identity heuristics, and other inferred-authentication models. These systems currently allow banks and platforms to construct an illusion of precision while erasing the harm experienced by fraud victims, especially the elderly, non-native speakers, migrants, and individuals targeted by phishing or impersonation.

The technologies of digital identity should not be a legal firewall. They should be interrogated, auditable, and always subject to challenge. **We call for the closure of a deliberate gap in fiscal responsibility that allows identity systems to be used as a shield against accountability.** If identity can be simulated, spoofed, or stolen, then legislation must treat it as fallible, especially when justice depends on it. ✳

Introduce biometric opt-outs and mandatory alternative access paths

Biometric and behavioural identity systems are now embedded in the infrastructure of civil life. From tax and welfare systems to health portals, visa applications, and public education, individuals are increasingly required to submit biometric or biometric-adjacent data to access basic rights and entitlements. These systems are typically presented as neutral upgrades to service delivery. In reality, when no alternative paths are provided, they are choke-points for failure and service denial.

We recommend that any digital identity system used to access civil services be required by law to offer non-biometric alternatives that provide equivalent functionality, access, and protection. This includes systems used for taxation, welfare, health care, immigration, public housing, voting registration, and education. Opt-out pathways must be non-punitive, permanent, and explicitly protected in both law and implementation. Users must not be forced to surrender biometric data or perform behavioural identity rituals simply to exist within a public system.

Despite claims to the contrary, biometric access is far from universal. This fact, coupled with the mutability of bodies over time, creates an ever-moving potential "edge case" for biometric failure. Our research shows that biometric systems are highly vulnerable to misclassification, coercion, and theft. When deployed at scale, digital identity systems that rely on biometrics disproportionately fail marginalised communities, including trans and gender-diverse individuals, people with disabilities, ageing populations, specific socio-economic classes, and those with religious or cultural objections.

The consequences of enforced biometric systems are not hypothetical. The single biggest example of this failure is also the most compelling and painful: individuals excluded from India's Aadhaar system due to biometric mismatch have been denied rations and pensions, with some dying as a result. The failures of Aadhaar for example are widely explained as edge cases, but with an estimated 5% of India's total population directly at risk, this is a population of millions. **This is an unthinkable outcome for a modern digital system.**

By mandating biometric opt-outs and alternative flows, we restore accountability to institutions and shift the burden of proof away from the individual. We further recommend that procurement frameworks, service design standards, and platform regulations prohibit single-channel biometric dependency. Wherever biometric systems are implemented, equal and clearly documented alternatives must exist, and they must be maintained and governed to the same standard.

No digital identity system should force the body into submission as a condition of receiving care, recognition, or aid. Refusal and alternatives must be a right. ✳

Enforce human-in-the-loop mechanisms for critical identity access pathways

Digital identity systems increasingly determine access to core services across both public and private sectors, from healthcare and banking to telecommunications, housing, and welfare. Each of these human systems use digital identity profiles to make automated decisions about who is allowed to access, modify, or control an identity,often without meaningful human oversight or recourse. When these systems fail or misclassify, users are left trapped in opaque procedures, flagged by opaque models, or denied access outright.

We recommend that all identity systems capable of granting or denying significant access – especially in contexts involving dependency, custody, financial exposure, or institutional power – be required to include qualified, independent human oversight for any automated decision-making. This includes both *denial events* (e.g. lost password or MFA, failed biometric verification, identity mismatch, guardianship challenge) and *assignment events* (e.g. custodianship activation, risk scoring, automatic delegation).

The absence of meaningful human review in critical identity pathways is a well documented source of harm. Previous events to address problematic or catastrophic assignment events, such as automatic risk scoring, eligibility decisions, and delegated authority, are mostly ineffective. The European Union's Right to Object legislation offers little practical recourse, and years of investment into "AI ethics" initiatives have yet to produce tangible protections for people navigating these systems. The architecture of automation has outpaced the institutions meant to mediate it. Such failed interventions are executed against a backdrop of ongoing and utterly unnecessary harm: Individuals denied healthcare due to facial verification errors, migrants refused boarding due to automated travel authorisation failures, parents locked out of support systems because of unreviewed profile mismatches, or survivors of domestic violence flagged by behavioural biometrics and denied service due to "suspicious" patterns. Each of these are designed as edge cases, but because they all trigger the same patterns through identity, they combine to become systemic outcomes.

The solution is to embed the right to human redress by design, a human-in-the-loop system that is qualified to interpret the context of the decision, override the system's default, and provide a clear resolution path. In high-stakes situations, such as guardianship disputes, involuntary health interventions, or financial disqualification, the human review must be timely, traceable, and independent from the initial system operator.

At the same time, transparency requirements for these interventions must be context-sensitive. In some cases, such as healthcare or child custody, privacy may preclude full audit trails. In others, like financial exclusion or benefit denial, users should have visibility into decisions made and the right to challenge them. Identity systems must be designed to accommodate both.

Proponents of digital identity often claim that human intervention creates inefficiencies, yet this has been repeatedly and demonstrably proven false. The absence of human oversight has produced higher error rates, greater administrative costs, and widespread harm that often requires complex remediation after the fact. Human-in-the-loop is an accountability mechanism. Without it, digital identity becomes a one-way system: perform or be excluded, comply or vanish. The ability to intervene, explain, and overturn decisions is essential to any identity infrastructure that claims to serve people rather than institutions.

Finally, despite frequent claims that human oversight invites corruption, our research shows the opposite: meaningful human intervention reduces social engineering risk by enabling contextual review, pattern recognition, and relational accountability. In contrast, digital identity systems that shift the burden of proof onto individuals without human mediation create the conditions for corruption within service providers, by allowing discretion and failure to hide inside automated systems with no audit or appeal. **In the absence of human accountability, where the burden of proof falls to the individual, coercion thrives.**

In environments where identity determines access, trust cannot be automated. There must always be someone to talk to, someone with the authority to make it right. ✳

Legislate platform obligations around disconnection and erasure

Modern digital platforms are embedded in systems designed to remember. Even when users delete their accounts, identity tokens often persist in shared spaces, linked data models, or cached systems. This creates an environment where disconnection is performative, and erasure is incomplete. In a highly adversarial new normal, this situation is particularly destabilising.

We recommend the introduction of legal mandates requiring all platforms that store or manage user identity,including social media, cloud services, fintechs, public infrastructure portals, and identity providers, to support total, irreversible disconnection and credential erasure at the user's request. This recommendation is universal in scope, It must apply to login credentials, federated identities, linked profiles, shared authentication tokens, and cryptographic keys used in delegated or shared access. All users, regardless of reason, must have the right to sever digital identity ties with platforms, other users, linked services, and ambient data relationships. The absence of this right has already enabled wide-scale harm: individuals fleeing abusive relationships, whistleblowers targeted through linked metadata, users unable to escape facial recognition logs or behavioural profiling. In high-risk contexts, such as intimate partner violence, digital coercion, stalking, or state surveillance, lack of disconnection is a material danger. More broadly, identity permanence enables dragnet surveillance tactics by U.S. Immigration and Customs Enforcement and other authoritarian regimes worldwide, making the inability to disconnect a universal risk.

This right must not be undermined by platform incentives, data retention defaults, or claims of technical infeasibility. We must reject the logic that immutability is a feature. If a user cannot revoke an identity, then the system is coercive by design. If a user cannot disconnect a credential from a platform, from another person, or from a history of interactions, then that credential is a liability.

All jurisdictions must introduce binding legislation that recognises disconnection and erasure as a foundational right of digital identity. This includes the right to:

- Permanently sever any identity credential, profile, or link, without requiring external authorisation;
- Remove persistent identifiers (e.g. phone numbers, biometric hashes, device IDs) from shared systems;

- Trigger erasure in crisis contexts with no requirement to prove harm;
- Access this right even in systems that claim immutability or distributed design (e.g. blockchain identity providers).

The inability to disappear must be treated as an unwanted and dangerous by-product of modern infrastructure. A platform that does not allow disconnection is a system of unending surveillance; A credential that cannot be revoked is a guaranteed future threat vector. ✳

Invest in defence systems at a consumer OS-level

Despite carrying the most sensitive credentials and mediating messages, video calls, authentications and other personal interactions, all operating systems act as a ‘neutral’ surface that can facilitate impersonation, coercion, and social engineering attacks at scale. Default behaviours often strengthen attack vectors rather than mitigate them. Tools that could scramble identity performance, block attribution, or signal duress are rarely implemented.

We recommend that major OS vendors, including Apple, Google, Microsoft, and Linux distributions, treat the defence against social engineering and identity manipulation as a first-order design priority. This means building and deploying operating system features that actively resist impersonation, phishing, and coercion. It also means removing or redesigning OS-level features that expose users to identity-based attacks, particularly those that falsely imply trust, reduce scepticism, or leak behavioural patterns.

Features that should be evaluated for redesign or removal include:

- Contact inference systems, such as iOS’s “Maybe: [contact name]” feature in iMessage and Mail, which suggest unverified identities based on name similarity, creating a false trust channel that directly assists impersonation;
- Smart notifications, which expose verification codes, security alerts, or session links on lock screens or in ambient UI layers, enabling shoulder surfing or screenshot-based attacks;
- Biometric unlocks under duress, which cannot distinguish coercion from consent and offer no fallback mechanisms for escape or recovery;

- Deep linking into financial or identity apps from messaging platforms, search, or web views, often triggered invisibly by URL preview or autofill features;
- Predictive autofill and name suggestions that override user intention, increasing the risk of credential stuffing and session impersonation;
- Overexposed accessibility or screen recording APIs, which allow sensitive information to be harvested under pretext or malware conditions, and;
- Predictive keyboard training and personalisation models, which can reveal behavioural signals and correlate identities across contexts.

We further recommend investment in *active defence features*, including:

- Real-time deepfake detection and user verification tools in video and voice calls, with user-controlled fallback to audio-only or text modes;
- Duress signalling mechanisms, allowing users to mark sessions as coerced and trigger alternate user interface states or communications;
- Metadata shielding, such as username-based routing (as adopted by Signal) to prevent phone number-based enumeration and coercion, and;
- Sandboxed identity modes, as pioneered by GrapheneOS, which allow for fully pseudonymous interaction at the OS level.

We recommend that OS vendors work with digital security researchers, intelligence officials, and consumer protection advocates to implement identity defence tooling as core infrastructure. This is a closing window of opportunity; If these systems are not cooperatively hardened at the OS layer, the opportunity to defend against identity manipulation will pass upstream into the hands of surveillance brokers, insurance risk engines, and adversarial state actors. **Digital identity is now adversarial by default. Our operating systems must behave accordingly.** ✳

Establish workplace identity sovereignty and analogue alternatives

Throughout this research project, we documented consistent efforts worldwide to roll out digital identity in the workplace. The scope is comprehensive: background checks, computer system logins, building access, HR accounts and employee monitoring beyond the hours of a full-time contract. Although these vendors promise efficiency and security, a systematic transformation of employment relationships into data extraction operations.

We have also documented how (and how frequently) workplace identity systems are weaponised to facilitate social engineering attacks, corporate espionage, harassment, and other adversarial purposes. Beyond external attackers, digital identity overreach by workplace leadership directly targets workers through surveillance. This practice accelerated dramatically during the transition to work-from-home and hybrid arrangements as COVID-19 behavioural patterns changed, manifesting as camera and software checks, keystroke surveillance and other intrusions into the home office.

This cannot continue. The dual-pronged attack on workers via surveillance from above and targeting from outside carries significant costs for an already atomised workforce. The modern workplace and its discontents directly contribute to downstream fracturing of social norms, productivity, and security, manifesting as “quiet quitting” as employees suffer workplace fatigue from employer overreach, to severe economic disruption from successful adversarial attacks that leverage worker identity systems as convenient entry points into organisational infrastructure.

The stakes become clearer in conflict zones where employment must continue during active warfare, for example the Ukraine-Russia conflict. Direct targeting of employee identity systems paralyse companies and destroys the livelihoods of those caught in the crossfire. Given current geopolitical trajectories, we believe this pattern will likely become more common as we transition into a period of localised proxy flashpoints for wider tensions. **The workplace, in other words, has become a battlefield where workers serve as unwilling intelligence assets.**

We reject the premise that digital identity is an non-negotiable dependency for modern employment. We recommend that all employers be legally required to maintain fully functional analogue alternatives for essential workplace operations, backed by legislative frameworks that treat worker identity sovereignty as a fundamental right rather than a technical accommodation.

Mandatory analogue alternatives must include:

- Physical timekeeping systems that do not require biometric verification or device interaction;
- Key-based or badge-based facility access that cannot be used for location tracking

- Direct deposit or cash payment systems that do not require smartphone apps or biometric verification;
- Human-conducted performance evaluations that cannot be supplemented by algorithmic behavioural analysis, and;
- Hiring processes that rely on interviews, references, and demonstrated skills rather than algorithmic screening of digital profiles.

These alternatives must be maintained indefinitely and funded at the same level as digital systems. Employers cannot be permitted to degrade analogue options to coerce digital adoption, nor can they impose administrative burdens that make refusal practically impossible.

Workers have the right to remain analogue without consequence, and we assert that this right includes protection from targeting by adversaries through reduced attack surface area, as well as freedom from direct targeting by leadership based on digital identity refusal. Union organisers, political activists, and other workers who face heightened surveillance risks must be able to maintain employment without exposing themselves to additional monitoring or targeting.

The workplace must not become a laboratory for identity surveillance nor a vector for information-powered warfare. Employment is too essential to survival to be held hostage by systems that treat human beings as data sources. We call on employment bodies and legislators to understand the structural inequalities inherent in employment-based digital identity and move decisively to reverse the rapidly colonised and precarious digitised employee. ✳

Deploy enforceable accountability systems to combat digital identity harms

From identity theft to system failures, digital identity consistently places responsibility on individual users rather than the institutions that design fundamentally vulnerable systems. “User sovereignty,” here described as a kind of freedom, create an exact power imbalance that make sovereignty impossible: Users receive theoretical control over credentials they cannot meaningfully protect, in systems they cannot audit, with recourse they cannot afford.

The consequences range from people starving after falling through digital welfare verification gaps to sophisticated money laundering operations that exploit the same verification systems meant to prevent them. Whether these outcomes result from incompetence or malice becomes less relevant as digital identity systems become more weaponisable and the stakes continue to escalate.

We recommend the introduction of comprehensive legal frameworks that assign direct liability to corporations whose systems enable identity-based harm across all sectors determining access to essential services, and to actors that leverage digital identity for fraud, discrimination or abuse. Companies marketing "self-sovereign" or "privacy-preserving" alternatives cannot exempt themselves from comprehensive liability while building business models that depend on the same extractive relationships with user data. Claims of platform neutrality must be legally rejected when systems actively enable discrimination, fraud, or violence. The accountability gap that allows profits to be privatized while harm is socialised must close. **The level of trust these systems demand should result in proportional scrutiny of both technical failures and unintended social consequences.**

Legislative response must include media training and standards guidelines that properly describe digital identity's negative outcomes, plus broader education in evaluating situations without disconnecting cause from effect. Without accountability, none of our other recommendations to strengthen digital identity systems become possible. ✳

Recognise Indigenous data sovereignty and governance authority

Digital identity systems imposed by settler states represent the latest iteration of a centuries-old colonial project: the systematic replacement of Indigenous governance with administrative systems designed for state control and surveillance. These systems flatten millennia-old kinship networks, sophisticated governance structures, and Indigenous ways of knowing into categories that serve invasive institutions rather than Indigenous self-determination.

What emerges is a particularly insidious form of digital colonialism, where the language of inclusion and modernisation disguises the continued erosion of Indigenous sovereignty.

We recommend that all levels of government formally recognise Indigenous peoples' absolute authority over identity governance within their territories and

communities. This includes the legal right to reject imposed digital identity systems, to design identity frameworks according to Indigenous laws and protocols, and to refuse participation in settler state identity infrastructures without loss of services, rights, or recognition.

Indigenous communities possess sophisticated governance systems that predate colonial contact by millennia – systems that include complex protocols for recognition, kinship determination, territorial relationships, and community membership that operate according to Indigenous law rather than settler legal frameworks. Digital identity systems treat Indigenous peoples as individual data subjects rather than members of sovereign nations with their own governance protocols. Digital identity, derived from Cybernetics, cannot capture the relational nature of Indigenous identity, which is often determined through kinship networks, testimony, community recognition, and territorial relationships rather than biological markers or administrative records.

Legal frameworks must be established that:

- Recognise Indigenous nations' exclusive jurisdiction over identity determination within their territories;
- Prohibit the extension of settler digital identity systems into Indigenous territories without explicit consent from Indigenous governments;
- Establish legal mechanisms for Indigenous communities to opt out of settler identity infrastructures while maintaining access to services and rights;
- Support Indigenous communities in developing identity governance systems according to their own protocols and technologies, which may include traditional practices, Indigenous-designed digital systems, or hybrid approaches determined by Indigenous communities themselves;
- Protect Indigenous data from extraction, linkage, or sharing with settler institutions without explicit Indigenous consent and governance oversight, and;
- Ensure that Indigenous peoples can maintain their citizenship and territorial rights regardless of participation in established identity systems.

Contemporary digital society cannot continue to impose identity systems designed for control while claiming to respect Indigenous rights. **Any identity system deployed within a society must exist alongside recognition of Indigenous nations as the**

rightful authorities over their own people, territories, and governance systems, including Indigenous authority over the fundamental question of identity itself, and the configuration of the state to accommodate for these determinations. ✳

Mandate universal bodily inclusion or reject digital identity systems entirely

Digital identity systems systematically exclude disabled people through design assumptions that treat certain bodies and minds as standard while relegating others to accommodation pathways. Throughout our research, we observed how biometric systems routinely fail disabled users: fingerprint scanners exclude amputees, workers who endure extreme conditions, and those with skin conditions. Facial recognition fails to recognise disabled faces or assistive devices, voice recognition discriminates against speech disabilities, and behavioural biometrics pathologise neurodivergent patterns as fraudulent. **The inability of a digital identity to represent a disabled person is presented as an edge case, but collectively exclude vast populations from essential services.**

On the other hand, “alternative pathway” offerings often come with extreme baggage that reinforces exclusion while placing adaptation burdens on disabled people. Accommodation processes are typically more burdensome, less private, and subject to discriminatory human judgment. They preserve the underlying systems that create exclusion while signalling that disabled people are problems to be managed rather than citizens entitled to equal access.

We call for mandatory total inclusion standards for any digital identity system proposed for public deployment, with systems that exclude any percentage of the population based on physical difference, cognitive variation, or neurodivergent patterns categorically rejected as discriminatory infrastructure:

- Any digital identity system must achieve universal accessibility across the full spectrum of human bodily and cognitive diversity as a prerequisite for approval;
- Systems that cannot serve disabled users must be abandoned rather than supplemented with accommodation pathways;
- Disabled people must have decision-making authority over any system affecting their access to services, including the right to reject systems entirely;
- Universal inclusion requirements must be enforced through independent audit with disabled community oversight, and;

- Alternative approaches such as human-mediated systems, relationship-based recognition, and context-specific identification must be prioritised when technological solutions cannot achieve universal access.

Given the stated goal of digital identity to be a representation of the human self in a networked world, it is completely unacceptable for any edge case to exist. If a system cannot be designed to work for every human body and mind, then it cannot be deployed at all. It is time for such systems to be held to this standard, or discarded as wholly unfit for its proposed purpose. ✳

Fund policy research into coercion, identity, and automation

Digital identity systems are political terrain that shape who is visible, who is credible, and who is vulnerable. As the conditions of the wider world deteriorate, how digital identity interacts with unstable conditions remains critically under-researched, particularly in its most urgent dimensions: coercion, consent, automation, and adversarial misuse.

We recommend the immediate and sustained funding of adversarial, socio-technical research into the evolving relationship between digital identity, coercion, and automation. This research must not be led by platform-aligned academics or policy consultants. As digital identity is shaped by market forces and the objectives of its designers, true interventionist research must be shaped by those who understand infrastructure as a site of control, who bring digital security methodologies into socio-technical contexts, and who operate with enough independence to hold both state and market accountable. Priority research areas should include:

- Defence capabilities against identity coercion at the OS and platform level;

- Viable alternatives to biometric dependency, particularly for at-risk populations;

- New forms of identity infrastructure that resist impersonation and social engineering;

- The role of digital identity in environments of institutional collapse, conflict, and forced migration, and;

- The use of identity systems in modern warfare, where digital traceability acts as an aggravating factor in atrocity, targeting, and disinformation.

This research should form the baseline for any identity system deployed at scale in digitised societies. Without it, policies claiming to serve human dignity will continue to be built on brittle assumptions. The urgency is clear. The European Union's Digital Identity Framework and Digital Sovereignty strategy cannot proceed without recognising this gap. Intelligence agencies, financial actors, human rights investigators, and aligned funders, especially those no longer convinced by platform optimism, must treat this as foundational research, not auxiliary inquiry.

Digital identity makes brittle digital societies. It introduces opportunity for failure states into every layer of social, economic, and civic infrastructure. In a multipolar world already defined by balkanisation, supply chain insecurity, and belligerent computational power. The question now is whether we are willing to fund the institutions necessary to understand, constrain, and outmanoeuvre them. ✳

Acknowledgements

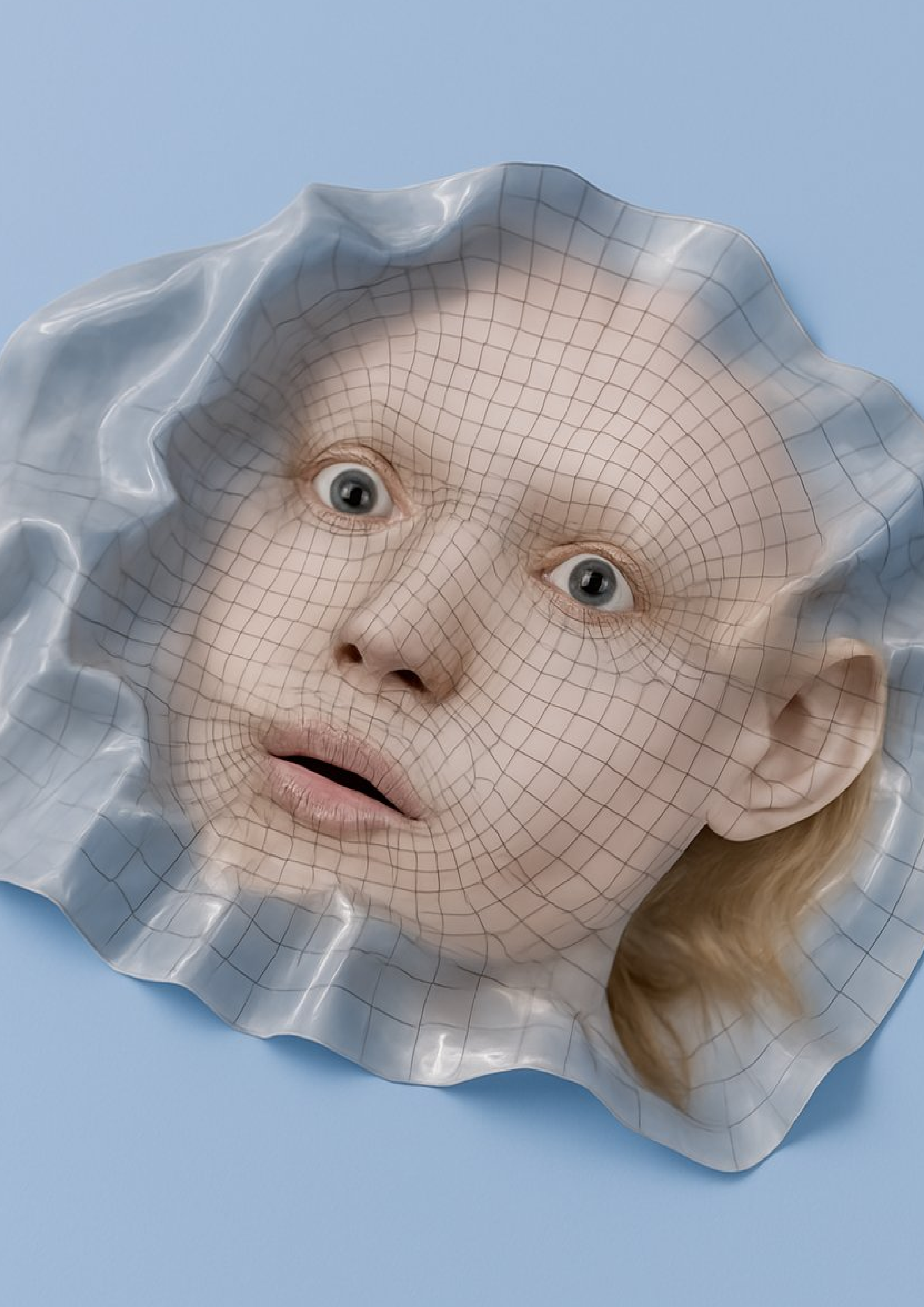
Researched and authored by Cade Diehm and Benjamin Royer and edited by Rocío Armillas Tiseyra and Rose Regina Lawrence. Roel Roscam Abbing co-authored Problem Statement III and provided extensive feedback for the report. Artwork by Ignatius Gilfedder and Cade Diehm.

The authors wish to acknowledge Esra'a Al Shafei, Dan Girshovich, Peter van Hardenberg, Matthew Canham, Meredith Whittaker, Matt Bailey, Caroline Sinders, John Marshall, Tian Tse, Eriol Fox, Teresa Zolnierkiewicz, Eleftherios Diakomichalis, Elio Qoshi, Laura Summers, Ilya Kreymer, Elys Day, Louis Center, Brent Bailey, Sandro Herbig, Dietrich Ayala, Danielle Brathwaite-Shirley, Allen "Gunner" Gunn, Aljoscha Meyer, Sammy Gwilym, Joe Hunting, Andrew Sempere, Chad Kohalyk, Cent Hosen, and participants.

This research was supported directly an indirectly via collaborations and/or grants from the following entities, in line with our Research Methodology and expectations of research independence:

- Signal Foundation
- Ink & Switch
- Public Office
- Radicle Foundation
- Aspiration
- Tools For Humanity
- Digital Credentials 4 Europe
- International Foundation for Electoral Systems
- Earthstar
- and 102 members of the NDCcommunity

New Design Congress (DE, UK, JA) is an independent research organisation confronting the gap between what is said to be happening and what is actually happening in digitised societies. NDC conducts critical and adversarial research into technology, politics and infrastructure, challenging prevailing assumptions about digital systems and their social impacts. Through rigorous investigation of platform governance, algorithmic mediation, and network vulnerabilities, the organisation publishes policy analysis, field research, economic theory, and experimental products that surface the material realities beneath technological rhetoric, and documents how digital dependencies shape contemporary power relations. Working with communities, institutions, and researchers globally, NDC creates tools and concepts for navigating digital precarity while advocating for alternative approaches to technological development that prioritise human agency and dignity in an unstable, uncertain world. ✳



Appendices

Appendix A. Glossary of terms

Account Takeover (ATO)

A form of identity fraud where an attacker gains unauthorised access to a victim's online account (often by stealing or guessing login credentials) and then exploits that access for malicious purposes.[503]

Accretionary ID Models

Identity systems that start with minimal evidence and build up identity information over time through accumulated validations and transactions. An individual can self-assert a basic identity with little or no initial documentation, and then gradually add verified attributes or attestations as they engage in various activities.[504]

Air-Gapped Device

A computer or device that is physically isolated from any network (internet or other external connections), ensuring it cannot be remotely accessed by attackers. Any data transfer to or from an air-gapped device requires manual methods (like using a USB drive), which greatly reduces exposure to malware and hacking. This extreme measure is often used to protect highly sensitive information or critical infrastructure from online threats.[505]

Algorithmic ID

An approach to identity verification where algorithms infer a person's identity or creditworthiness from their digital behaviour and patterns, rather than from fixed government IDs or one-time biometrics. For example, a financial service might authenticate or assess a user by analysing their ongoing transaction history, social media usage, or mobile phone habits.[506]

[503] Internet Crime Complaint Center (IC3). *Account Takeover Fraud* (ATO). Federal Bureau of Investigation (FBI). Accessed 12 May 2024, https://www.ic3.gov/CrimeInfo/AccountTakeover.

[504] Al Tariq Sheik et al. "A Comparative Study of Cyber Threats on Evolving Digital Identity Systems." In *Proceedings of the 2021 IET International Conference on Biometric Engineering and Applications*, 352-360. Institute of Engineering and Technology, 2021, https://www.researchgate.net/publication/357010099_A_Comparative_Study_of_Cyber_Threats_on_Evolving_Digital_Identity_Systems.

[505] *What Is Air Gap? Essential Guide to Air Gap Security.* Fortinet, accessed 8 September 2024, https://www.fortinet.com/resources/cyberglossary/what-is-air-gap.

[506] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development (Washington DC: USAID, 2017), https://www.ictworks.org/create-digital-id-inclusive-development/

ANXIETY Framework

A socio-technical adversarial threat analysis methodology that expands traditional cybersecurity threat modelling beyond purely technical categories to encompass infrastructural, political, psychological, and social attack surfaces within a unified analytical framework. The ANXIETY taxonomy comprises seven distinct threat vectors organised as an acronym structure: *Appropriation*, *Negligence, Exclusion, Impersonation, Exploitation, Toxicity* and *Yielding*.

Unlike conventional threat modelling frameworks, the ANXIETY Framework explicitly acknowledges the socio-technical entanglement of contemporary threats, where technical vulnerabilities intersect with political dynamics, social structures, and infrastructural dependencies.[507]

API (Application Programming Interface)

A set of rules and interfaces that allows different software programs to communicate. An API defines how one piece of software can request services or data from another in a standardised format. By exposing specific functions and data while keeping the rest encapsulated, APIs enable interoperability and integration across systems.[508]

Assetisation

The process of treating personal data or identity credentials as economic assets. Common in Web3, data brokerage and financial sectors. For example, companies may monetise user data, effectively "assetising" identity information by buying, selling, or leveraging it for financial gain. [509]

Assurances (Levels of Assurance):

TThe degree of confidence in identity processes, often aligned to frameworks (e.g., NIST SP 800-63) that separate: *Identity Assurance Level* (IAL) for proofing strength, *Authentication Assurance Level* (AAL) for how strongly a user is authenticated, and *Federation Assurance Level* (FAL) for token/transaction protection. Higher assurance may require supervised, in-person proofing and multi-factor authentication; lower assurance may accept self-asserted data or a single factor.[510]

[507] Cade Diehm, "ANXIETY Framework History - from 2016-2025," *Anxiety.Games*, August 2025, https://anxiety.games.

[508] Microsoft Learn. "Introduction to APIs." Updated 7 February 2024, https://learn.microsoft.com/en-us/xandr/industry-reference/intro-to-apis.

[509] Lili Chen. "Data Assetization and Capital Market Information Efficiency: Evidence from Chinese A-Share Listed Companies." Future Business Journal 9, 2023, https://fbj.springeropen.com/articles/10.1186/s43093-024-00401-w.

[510] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special

Attacker Model

A description of the potential attacker's capabilities and methods that a security system is designed to defend against. Also known as a threat model or adversary model, it outlines what the attacker is assumed able to do – for example eavesdropping on networks, guessing passwords or corrupting insiders – and their goals as an adversary.[511]

Attestation

An authoritative, usually cryptographically signed statement that a claim about a person or device is valid. Examples: a university issues a degree attestation; a device produces device attestation proving it is genuine and untampered. In verifiable-credential systems, attestations are the signed claims inside credentials.[512]

Attribute

A piece of information about a person or entity that can be serialised and used to describe or identify them. Attributes include core traits (name, date of birth, biometrics) and descriptive data (email, job title, qualifications). In digital identity, attributes are the building blocks used to confirm ownership of an identity and to grant access when policy conditions are met.[513]

Attribute Assertion

A statement or claim about an attribute of an individual ("*this person has attribute X with value Y*"), usually made by an authoritative source and often in a digitally verifiable format, and typically shared as part of authentication or authorisation flows. For example, a government might provide an attribute assertion that *"Nationality = Canadian"* for a citizen, or an employer asserts *"Employment Status = Current"* for an employee.[514]

Attribute Authority

An organisation or service that is trusted to validate and issue attributes about individuals. For instance, a motor vehicle department is an attribute authority for driver's license status, and a university is an authority for education credentials. When an attribute

Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

[511] Pratyush Kumar et al. "A Formal Analysis of SCTP: Attack Synthesis and Patch Verification." arXiv January 2024, https://arxiv.org/html/2403.05663v1.

[512] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

[513] World Bank, "Attribute," In *ID4D Glossary*, 2023, https://id4d.worldbank.org/guide/glossary.

[514] Authentication and Authorisation for Research and Collaboration [AARC], *Terms and Definitions*, 2024, https://aarc-community.org/training/terms-and-definitions/.

authority provides an assertion (e.g. *"Ripley's role is 'Student'"* or *"Kodak's age is 25"*), requesting parties accept it as true because of the authority's standing and the secure way the assertion is delivered.[515]

Attribute-Based Access Control (ABAC)

An access control model that grants or denies access based on attributes associated with the user, the resource, and the context, rather than fixed roles or lists of permissions. Under ABAC, policies are written as rules evaluating attributes. For example, *"Allow access if user.department = HR and resource.type = Payslip and time = work_hours."* Because decisions are made by evaluating attribute values against policy rules, ABAC is very dynamic and flexible: changing an attribute automatically changes their access rights, without needing to edit specific access control lists.[516]

Authentication

The process of verifying an identity claim to confirm that a user or entity is who they say they are, and a cornerstone of security: only after authentication can a system safely grant personalised access or privileges. In practice, authentication is achieved by checking some form of credential or proof provided by the user against the expected credentials. Common methods include entering a password (something the user knows), providing a biometric like a fingerprint or face scan (something the user is), or presenting a smart card (something the user has). Successful authentication gives a level of confidence that the entity interacting with the system is the legitimate, previously enrolled subject.[517]

Authentication (Inherence Based)

An authentication factor using inherent physical or behavioural characteristics (e.g., fingerprint, facial recognition, iris, voice, gait). Example: unlocking a phone with a thumbprint.[518]

Authentication (Knowledge Based)

An authentication factor that uses knowledge known only by the user to verify their identity, usually a secret such as password or PIN, which the user memorises and provides

[515] Authentication and Authorisation for Research and Collaboration [AARC], *Terms and Definitions*, 2024, https://aarc-community.org/training/terms-and-definitions/.

[516] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

[517] World Bank, "Authentication," In *ID4D Glossary*, 2023, https://id4d.worldbank.org/guide/glossary.

[518] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

during login. Other forms include security questions ("What was your first pet's name?") or one-time passcodes delivered to users if those are considered knowledge, though often they're classified separately.[519]

Authentication (Multi-factor Based)

Authentication that uses two or more distinct factor categories (knowledge, ownership, inherence). Example: bank card (have) + PIN (know).[520]

Authentication (Ownership Based)

An authentication factor based on something the user has, such as a smart card, a FIDO2/WebAuthn security key, or a one-time-password (OTP) generator. These devices generate or hold secrets and perform cryptographic challenges.[521]

Authentication (Zero-Knowledge Based)

Authentication where a user proves knowledge of a secret or satisfaction of a condition via zero-knowledge proofs without revealing the secret itself, improving privacy and reducing exposure. Central to this approach is the use of mathematical zero-knowledge proofs, which are cryptographic protocols allowing one party (the prover) to convince another (the verifier) that they know a value (like a password or key) or satisfy a condition, without ever sharing the actual value.[522]

Authorisation

The process of granting or denying access to resources or actions after successful authentication, typically using the principle of least privilege through roles, attributes, or policies. In other words, if authentication is the process of 'gatekeeping' a user until they successfully prove they own a digital identity, authorisation decides what the user is able to access within a system with the digital identity. For example, after logging in, a user might be authorised to view their own account information but not someone else's, or an employee might be authorised to edit documents but not delete them. Proper authorisation

[519] World Bank, "Authentication," In *ID4D Glossary*, 2023, https://id4d.worldbank.org/guide/glossary.

[520] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] (Gaithersburg, MD: National Institute of Standards and Technology, June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

[521] World Bank, "Authentication," In *ID4D Glossary*, 2023, https://id4d.worldbank.org/guide/glossary.

[522] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] (Gaithersburg, MD: National Institute of Standards and Technology, June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

ensures the principle of least privilege is enforced, so users only access information and functions necessary for their role. These can also known as permissions.[523]

Backdoor

An undocumented or secret method of bypassing normal authentication and security controls to gain unauthorised access to a system, usually without tripping the system's defensive capabilities. Backdoors can be deliberately built in (for example, a developer leaves a hidden login account for maintenance) or introduced maliciously (through malware that opens a hidden access point for attackers). Because backdoors avoid the usual protective checks, they pose a serious security risk: anyone who discovers the backdoor can exploit it to enter the system at will.[524]

Behavioural Biometrics

A way of determining biometric components of a digital identity using patterns in a user's behaviour rather than their physical traits. Behavioural biometrics leverage the unique ways individuals perform activities, such as how a user types, how they hold their phone, how they walk, or their browsing patterns. Over time, systems can build a profile of these behaviours and continuously authenticate a user by detecting anomalies that could indicate the hijacking of an identity by an attacker.[525]

Biometric Poisoning

A type of attack where someone corrupts or manipulates biometric data or systems in order to undermine their reliability or to impersonate someone by injecting additional, unrelated biometric data into the credential. In essence, the attacker "poisons" the biometric data or model, by introducing subtly altered fingerprint records, feeding malicious training data to a facial recognition AI, or incrementally biasing a system's stored credential. The goal might be to trick the system into false acceptances when provided with specific, unauthorised biometrics, or to cause false rejections that lock out the legitimate user by distorting their stored template. Once poisoned, it is often extremely difficult to repair poisoned biometric data without resetting the credential altogether.[526]

[523] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development [Washington DC: USAID, 2017], https://www.ictworks.org/create-digital-id-inclusive-development/.

[524] National Institute of Standards and Technology, "Back Door," Computer Security Resource Center Glossary, https://csrc.nist.rip/glossary/term/backdoor.

[525] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

[526] Biometric Backdoors: A Poisoning Attack against Unsupervised Template Updating," in *Proceedings of the 2020 IEEE European Symposium on Security and Privacy* [EuroS&P 2020], 2020, https://ora.ox.ac.uk/objects/uuid:8f12be84-01f4-47c3-83c9-c08ac53eee8a.

Biometrics

Measurement of physical or behavioural traits for identification or authentication (e.g., fingerprints, face, iris; voice, gait, typing rhythm). Common physical biometrics include fingerprints, facial features, iris or retinal patterns, and DNA; behavioural biometrics include voice, gait, and typing rhythm. The premise is that these traits are highly distinctive for each person and generally stable over time, so they can serve as a natural password that a user always carries. Biometric systems capture a sample and match against stored templates. Strengths include convenience and difficulty of sharing; risks include presentation attacks, bias, sensor quality issues, and irrevocability (you cannot change your fingerprints if leaked).[527]

Binding

The practice of firmly associating an identity credential with the correct individual. During the enrolment process, once a person's identity is verified, the system "binds" their credential, such as a username, smart card, or a digital certificate, to that person's identity record. For example, when you get a passport, your biometric and personal details are bound to the passport document, ensuring that the document belongs uniquely to you. Binding can also describe the process of authorising an account to a particular device, like binding a token to a user's phone.[528]

Blockchain

A decentralised distributed database consisting of a chain of blocks containing chronologically correlated transactions validated by cryptographic algorithm. In a blockchain, many participants (nodes) maintain and validate the ledger collectively, rather than relying on a single central authority. Each block contains a batch of transactions or records, plus a reference (hash) to the previous block, forming an unbroken chain back to the first block (genesis block). This design makes the ledger tamper-evident: altering any past data would break the chain's cryptographic links, and consensus rules prevent unauthorised changes, such as attempts to introduce fraud or reassign transactions unilaterally. Blockchains underlie cryptocurrencies like Bitcoin, but also have non-currency uses such as tracking assets, executing 'smart contracts', and enabling decentralised identity.[529]

[527] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

[528] National Institute of Standards and Technology, "Binding," Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/binding.

[529] Agata Ciaburro, "Benefits and Use of Blockchain Technology to Support Supply Chain during COVID-19," in *Handbook of Statistics*, vol. 46: Data Science for COVID-19 [Amsterdam: Elsevier, 2022], 157-170,

Browser-Bound Credential

A credential or key tied to a specific browser/device environment such that it cannot be replayed elsewhere. Today this is most robustly achieved with WebAuthn passkeys (public-key credentials bound to origin and device, optionally synced securely across devices). Earlier "token binding" approaches at the HTTP/TLS layer exist but are largely deprecated in favour of WebAuthn.[530]

Brute-Force

A trial-and-error attack method used to crack passwords or keys by systematically trying every possible password or passphrase until the correct one is found. The term evokes the idea of using sheer force – in this case, computing power – rather than cleverness: the attacker "brutes" their way in by exhausting possibilities rather than researching and understanding a system and exploiting its vulnerabilities. Brute-force attacks can be used against passwords, PINs, cryptographic keys, or any other secret token and are often limited by the fact they are time consuming, and that modern systems limit the number of incorrect authentication attempts before requiring additional measures from the user. The most common method of a brute-force attack is to optimise the strategy by iterating through common passwords and dictionary words (see **Dictionary attack**) rather than working sequentially through every possible combination.[531]

CAPTCHA

An acronym for *Completely Automated Public Turing test to tell Computers and Humans Apart*, the CAPTCHA is a challenge-response test on websites used to differentiate real human users from bots or automated scripts. These are often deliberately awkward puzzles of distorted text, image clicks, and behavioural checks, inserted into a user flow to discriminate between a human user and an automated agent. CAPTCHAs act as a security gatekeeper on forms and login pages by requiring interaction that (currently) only humans are proficient at. However, as AI improves at solving these challenges, CAPTCHAs evolve as well to include behavioural analysis or more complex puzzles.[532]

https://pmc.ncbi.nlm.nih.gov/articles/PMC9347267/.

[530] Google Chrome Security Team, "Origin Trial: Device Bound Session Credentials in Chrome," *Chrome Developers blog*, 29 Sept 2023, https://developer.chrome.com/blog/dbsc-origin-trial.

[531] Cybersecurity and Infrastructure Security Agency, "CISA and Partners Warn Organisations of Brute Force Techniques," 7 July 2021, https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors.

[532] B Yan and G Zhao, "Strengthening CAPTCHA-based Web Security," First Monday 17, no. 7, 2012, https://firstmonday.org/ojs/index.php/fm/article/download/3630/3145.

Cartesian Identity / Rational identity

A concept of personal identity rooted in the philosophy of René Descartes – essentially viewing the self as a singular, indivisible "I," or the classic notion *"I think, therefore I am"*. Also known as the rationalist view of the self, the Cartesian identity assumes each person has a unified, core identity that remains constant and is the source of one's thoughts and experiences.[533]

Cartesian Identity / Rational Identity (Digital-Identity Context)

The assumption in information security, cryptography and digital identity systems that a single, self-contained subject can prove existence within a system merely by presenting the correct credential, echoing Descartes' rational identity claim, *"I think, therefore I am,"* in a digital way. In the context of digital identity, the claim extends into authentication as *I authenticate, therefore I am*, and further to *I curate, therefore I am* (presentation) and *I transact, therefore I am* (assetisation). While elegant for systems modelling, embedding Cartesian philosophy into digital identity abstracts away social context; the resulting trust gap ensures that social-engineering breaches will persist.[534]

Centralised Identity

A model where a distinct identity provider (IdP) manages design, authentication, and authorisation, and relying services integrate with it. One credential grants access across multiple services. This creates a power centre: the IdP becomes a gatekeeper for access, policy, and governance.[535]

Circle of Trust

In federated identity, a circle of trust is a group of parties, such as multiple organisations or service providers, that agree to honour each other's authentications and identity assertions. Within a circle of trust, one or more Identity Provider (IdP) and multiple Service Providers (SPs) cooperate, so a user authenticated by an IdP member can access services of another SP without re-authenticating at each service. All members have established mutual trust, often through legal agreements, standards, and shared security policies. Each SP and IdP commits to properly managing user identities and credentials. For example, in a university consortium, each campus might trust the others' logins – a student

[533] René Descartes, *Discourse on the Method*, trans. and ed. by Liz Opara (New Learning Online, 1637).

[534] See Problem Statement II.

[535] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

from campus A can use campus B's library system via federation because those campuses are in a circle of trust.[536]

Claim

A statement about an entity or person that is asserted to be true. It could be self-asserted or provided by another party. Examples of claims include *"Ripley's email is ripley@newdesigncongress.org," "Kodak is a certified engineer,"* or *"Citra's age is 30."* Claims often correspond to attributes, but the term "claim" is especially used in the context of verifiable credentials where an issuer makes claims about a subject that can be checked by a verifier.[537]

Cold Wallet

A cryptocurrency wallet stored offline, providing a high level of security for digital assets. The term "Cold" means it's not connected to the internet, thus safe from online hacking attempts. Cold wallets are often stored on USB-like hardware or on paper. Cold wallets are typically difficult to steal without physical access to the hardware/paper directly. Because the private keys are kept offline, an attacker cannot remotely steal the crypto — one would need physical possession of the wallet device or material.[538]

Conditional Pseudonymity

A privacy arrangement where a person operates under a pseudonym by default, but their real identity can be revealed under predefined conditions, for example legal or safety reasons. Conditional pseudonymity aims to balance privacy and accountability: users enjoy anonymity in general use, yet there's a mechanism to pierce the veil if absolutely necessary. A real-world analogy is a numbered bank account where the bank knows the owner but others only see a number, unless law enforcement compels disclosure.[539]

Consent

Permission or agreement given by an individual for something to happen, after having knowledge of what that entails. In the context of digital identity and data, consent means a person voluntarily approves the collection, use, or sharing of their personal information. In everyday digital identity interactions, consent is simply saying *"Yes, it's*

[536] ForgeRock, "OpenIG as a SAML 2.0 Service Provider," *Open Identity Platform* documentation, 2019, https://doc.openidentityplatform.org/openig/gateway-guide/chap-federation.

[537] Manu Sporny et al., "Verifiable Credentials Overview," *W3C Group Note*, 3 March 2020, https://www.w3.org/TR/vc-overview/.

[538] Nathan Reiff, "Cold Storage: Cryptocurrency Private Keys Stored Offline," Investopedia [updated 7 Dec 2024], https://www.investopedia.com/terms/c/cold-storage.asp.

[539] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development [Washington DC: USAID, 2017], https://www.ictworks.org/create-digital-id-inclusive-development/.

okay to do X” – like consenting to have one’s credit checked or to link accounts for identity verification – and without it, organisations should not proceed with those actions regarding personal data.[540]

Contextual Integrity

A principle of privacy developed by Helen Nissenbaum that holds that information is protected when it flows in a manner consistent with the social context’s norms and expectations. For example, an individual might freely give their medical information to a primary care physician because that context expects confidentiality and medical use only, but that same person would expect the healthcare provider to not share that data with a pharmaceutical marketer. Doing so would be a violation of contextual integrity.[541]

Continuous Authentication

Ongoing verification during a session using signals such as typing patterns, pointer movement, device posture, or location. If risk increases or anomalies are detected, the system can step-up authentication or terminate the session. [542]

Convention

An agreed-upon standard, norm, or formal agreement in the realm of digital identity. Examples include technical conventions or standard formats that all parties use for exchanging identity data, and legal/policy conventions, such as an international treaty or framework concerning digital identities. The “eIDAS convention” is often used to describe common regulations EU countries follow for electronic identification. Generally, a convention is something that stakeholders have collectively accepted so that systems or organizations can interoperate smoothly. It ensures everyone is on the same page regarding certain practices or definitions. In digital identity, adhering to conventions – whether it’s data schemas, security protocols, or user interface norms – promotes compatibility and trust between different systems and jurisdictions.[543]

Correlation

The practice of linking separate data sets that relate to the same person (deterministically or probabilistically). Useful for SSO and fraud detection, but risky for

[540] Regulation (EU) 2016/679, General Data Protection Regulation, art. 4(11), OJ 2016 L 119/1, https://gdpr-info.eu/art-4-gdpr/.

[541] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development (Washington DC: USAID, 2017), https://www.ictworks.org/create-digital-id-inclusive-development/.

[542] OneSpan, “Continuous Authentication: What It Is and How It Works,” *OneSpan Blog*, 2023, https://www.onespan.com/topics/continuous-authentication.

[543] Rainer Diaz-Bone, “Statistical Panopticism and Its Critique,” *Historical Social Research* 44, no. 2 (2019): 77-102, https://www.jstor.org/stable/26604899.

privacy when done without consent, as in cross-site tracking. Often this is used to deduce that User A in System X is the same individual as User B in System Y by matching identifying information. For example, if two services share a common identifier or enough attributes (like email plus birthdate), an observer could correlate those records and realise they belong to one person, thus aggregating information from multiple sources. [544]

Credential

A proof of identity or attributes that an individual possesses, used for authentication. Credentials can be anything physical or digital that serves as an "identification card" in the digital system. Common examples include a username/password combination (the credential being the knowledge of those), a digital certificate, a smart card, or a mobile authenticator app that generates time-based codes. The credential contains or provides access to the data that verifies you are who you claim to be – for instance, a passport is a credential in the physical world, and an SSL certificate is a credential for a website. In new or emergent identity paradigms, users might hold verifiable credentials (digital attestations) like "Proof of Age" or "Membership Status" which they can present on request. In all cases, the credential by itself isn't useful until a verifier checks it against an authority or its inherent validity, after which the user is granted access or rights based on it.[545]

Credential Issuing

The act of creating and securely delivering a credential after appropriate proofing and binding to the subject (e.g., issuing a passport, security key enrolment, or a verifiable credential). Good practice ensures integrity during generation and delivery and sets up lifecycle controls (renewal, rotation, revocation).[546]

Credential-Stuffing

A cyber-attack where stolen username/password pairs from breaches are automatically tried on other services to exploit password reuse. Effective defences: unique

[544] Stacie B Dusetzina, Seth Tyree, Anne-Marie Meyer, Adrian Meyer, Laura Green, and William R Carpenter, Linking Data for Health Services Research: A Framework and Instructional Guide, *Agency for Healthcare Research and Quality*, 2014, https://pubmed.ncbi.nlm.nih.gov/25392892/.

[545] National Institute of Standards and Technology, "Credential," *Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/credential.

[546] Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* [NIST Special Publication 800-63-3] [Gaithersburg, MD: National Institute of Standards and Technology, June 2017], https://pages.nist.gov/800-63-3/sp800-63-3.html.

passwords, strong password hashing at the server, MFA/passkeys, rate-limiting, and breach-password screening.[547]

Certificate (Digital Certificate)

An electronic credential, typically in the form of a small data file, that verifies the identity of an entity and binds it to a cryptographic key. Most commonly, certificates are most often encountered daily as SSL/TLS credentials offered by websites over HTTPS. The website presents an X.509 digital certificate to prove it is the legitimate site, like *https://newdesigncongress.org*, and that certificate is issued by a trusted third party called a Certificate Authority (CA). A certificate contains the subject's name or domain, their public key, an expiration date, and is digitally signed by the CA. If the signature is valid and the CA is trusted by a user's device, the general consensus is to accept that certificate as genuine. Certificates ensure secure communications via encryption, and trust in the opposite party. Certificates can also be used for code signing, email encryption, and personal digital identity cards.[548]

Custodian

A party holding or managing something for someone else with a duty of care (e.g., an exchange holding crypto keys in a custodial wallet; a cloud IdP storing credentials). The custodian must protect against loss or misuse and act in the owner's best interests.[549]

Cybernetics

An interdisciplinary science focused on communication and control in systems, whether those systems are machines, living organisms, or social organisations. The term was coined by Norbert Wiener, who defined it as *"the science of control and communication in the animal and the machine"*. Cybernetics looks at how systems self-regulate via feedback loops – for example, a thermostat uses feedback to control temperature, or an organism uses feedback from the environment to maintain homeostasis. Key concepts include feedback, adaptation, and goal-oriented behavior in complex systems. All forms of digital identity and information security are built upon cybernetic principles that are inherent in computing, covering everything from user behavior to information flows in a network, to the design of systems such that these can be controlled or directed.

[547] National Cyber Security Centre, "Use of credential stuffing tools" (London: NCSC, 19 November 2018), https://www.ncsc.gov.uk/files/Credential%20stuffing%20advisory.pdf.

[548] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russell Housley, and William Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Request for Comments 5280 (May 2008), https://www.rfc-editor.org/info/rfc5280.

[549] Uniform Law Commission, Revised Uniform Fiduciary Access to Digital Assets Act (2015) (Chicago: ULC, 2015), § 2 ("Definitions"), https://www.uniformlaws.org/viewdocument/final-act-with-comments-40?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22.

The principles of cybernetics underlie many modern technologies: machine learning algorithms adjusting outputs based on feedback, or network protocols controlling data flow.[550]

Data Broker Re-Identification

An attack scenario in which data that was supposedly anonymised or pseudonymised is matched back to specific individuals by aggregators or data brokers. Data brokers often collect and sell large sets of user data, such as web histories, location logs, purchase records, under a promise that such data is de-identified. However, through cross-referencing multiple datasets and using unique combinations of attributes, it's frequently possible to re-identify individuals, Re-identification defeats the purpose of anonymisation, leading to privacy violations where brokers or attackers reconstruct profiles of persons without consent. This practice is a significant privacy concern because individuals often have no idea how disparate pieces of their data can be combined to single them out.[551]

Data Minimisation

A principle (e.g., under GDPR) requiring that personal data collected/retained be adequate, relevant, and limited to what is necessary for the purpose. It also implies appropriate retention limits.[552]

Decentralised Identifier (DID)

A globally unique identifier for an entity (person, organisation, device, etc.) that is not dependent on any central authority, often used in the context of self-sovereign identity. DIDs are often resolved to a DID Document which contains public keys and service endpoints for that identity, enabling trustable interactions. Unlike traditional identifiers that belong to providers, such as email addresses or social media IDs, DIDs are controlled by the user/identity owner and typically recorded on distributed ledgers or similar decentralised networks. This makes them persistent, as they don't change or vanish if a company goes out of business. It also makes them verifiable via cryptographic confirmation of a DID's associations via its document. DIDs are a cornerstone of decentralised identity

[550] Norbert Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine* 2nd ed. [Cambridge, MA: MIT Press, 1961]. https://mitpress.mit.edu/9780262730099/cybernetics/.

[551] Latanya Sweeney, "Simple Demographics Often Identify People Uniquely," *Data Privacy Working Paper* 3 [Pittsburgh: Carnegie Mellon University, 2000], https://dataprivacylab.org/projects/identifiability/paper1.pdf

[552] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development [Washington DC: USAID, 2017], https://www.ictworks.org/create-digital-id-inclusive-development/.

initiatives: they allow users to prove things about themselves without always referencing a central registry.[553]

Deepfake

A highly realistic but fake piece of video, image, or audio created using AI techniques to impersonate someone's appearance or voice. The term comes from the portmanteau of "deep learning" and "fake." An attacker might generate a deep fake audio of a high net worth individual confirming the transfer of a significant sum in an attempt to convince others to complete the transaction. These are made with machine learning models (such as Generative Adversarial Networks) that learn to mimic the target from many samples. Deepfakes now pose serious risks to digital identity as they can be deployed adversarially to attack authentication (by generating partial or complete credentials that can pass validation) and presentation (by presenting a digital representation of a user or IdP/SP) layers of digital identity.[554]

Deepfake Voice Spoof

Also known as voice cloning, this cybersecurity attack is a specific type of deepfake where AI-generated audio mimics someone's voice, often used in a scam or spoofing context to deceive listeners or voice authentication systems. An algorithm is trained on recordings of a person speaking and can then produce new speech in that person's voice saying any chosen words. Attackers use this in social engineering attacks, for example, calling an employee while imitating the CEO's voice to authorise a fraudulent money transfer. Deepfake voice spoofs threaten voice-based two-factor authentication or verification steps.[555]

Delegation

The act of granting someone else the authority to act on your behalf in a specific context or task. Delegation might mean a user allow another user or a service to access certain resources or perform actions as if they were the requesting user. For example, in an identity context, you might delegate your assistant the right to approve certain requests in a system using your credentials, or a service might delegate authentication to an OAuth provider. Delegation is common in access management: one user or process is entrusted to

[553] World Wide Web Consortium (W3C), *Decentralized Identifiers (DIDs)* v1.0 W3C Recommendation (19 July 2022), https://www.w3.org/TR/2022/REC-did-core-20220719/.

[554] Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review 107, 2019, https://lawcat.berkeley.edu/record/1136469/files/2-Chesney-Citron.34.final_.pdf.

[555] Federal Communications Commission, "FCC Makes AI-Generated Voices in Robocalls Illegal," News Release (Washington, DC: FCC, 8 February 2024), https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal.

do something for another. To manage it safely, delegation is usually constrained – limited in scope and time (like giving someone power of attorney for a day, or an app a token to access your data for an hour).[556]

De-Duplication

The process of detecting and eliminating duplicate entries for the same person in an identity database. If one individual accidentally or fraudulently is enrolled twice under different IDs, de-duplication aims to spot that and merge or remove duplicates so that each real person corresponds to only one identity record. Techniques for de-duplication include comparing fingerprints or other biometrics across records, matching on combination of personal attributes, or using algorithms that flag records with high similarity. Ensuring uniqueness is crucial for integrity.[557]

Device Fingerprint

A (probabilistic) identifier built from a device's stable attributes (e.g., GPU, canvas quirks, fonts, time-zone). Used for adaptive authentication and bot mitigation, but raises privacy concerns due to opacity and persistence[558]

Device Reputation

Sometimes called a device risk score, device reputation builds on fingerprinting with historical and consortium data to judge whether a device (or cluster) has been linked to fraud or benign use, informing allow/challenge/deny decisions.[559]

Dictionary Attack

A targeted form of brute-force password cracking. Instead of trying every possible character combination, the attacker iterates through a curated list of common words, leaked credentials and predictable variants such as *Password1!* or *Summer2025*. Because many users choose easily memorised strings, dictionary attacks can compromise accounts quickly and with modest computing power. Defences include enforcing long, random pass-phrases, salting and stretching hashes, and rate-limiting login attempts.[560]

[556] OASIS, XACML v3.0 Administration and Delegation Profile Version 1.0 OASIS Committee Specification 01, edited by Erik Rissanen (10 August 2010), https://www.oasis-open.org/standard/xacml3-0-admin/.

[557] Shruti Trikanad and Amber Sinha, "Digital Identities: Design and Uses", 2019, https://digitalid.design/core-concepts-processes.html.

[558] Lorenzo Casini, Measuring the Adoption of Device Class Fingerprinting (MSc thesis, Radboud University, 2024), https://www.cs.ru.nl/masters-theses/2024/L_Casini___Measuring_the_Adoption_of_Device_Class_Fingerprinting.pdf.

[559] Laatansa et al., "Password Cracking with Brute Force Algorithm and Dictionary Attack," *Applied Sciences* 13, no. 10 (2023),https://www.mdpi.com/2076-3417/13/10/5979.

[560] GlobalData, "Digital Identity – Thematic Intelligence," *GlobalData Plc*, 11 November 2024,

Digital Identity Value Chain

The digital identity value chain maps the full journey of an identity from initial proofing to retirement. Typical stages are:

1. Proofing & Enrolment designed to verify the subject and issue credentials;
2. Binding linking authenticators, such as passwords, cryptographic keys, biometrics;
3. Credential Management via secure storage, rotation and revocation;
4. Authentication flows to prove control of the credential during service access;
5. Authorisation & Attribute exchanges that provide verified attributes to relying parties, and;
6. Lifecycle operations, typically update, merge, suspend or delete, that help manage the identity.

Each link creates economic value but also introduces distinct trust and privacy risks.[561]

Digital Shadow

Also called a passive digital footprint, a digital shadow is the sum of data fragments an individual or organisation leaves behind simply by existing in networked environments: server logs, metadata, loyalty-card records, CCTV images, location pings and more. Unlike an intentional 'digital twin', the shadow is assembled by third parties; it can be aggregated to infer sensitive attributes or predict behaviour. Limiting one's shadow involves data-minimisation, strict retention schedules and exercising data-subject rights under laws like the GDPR.[562]

Disambiguation

The process of resolving ambiguity when two or more records, identifiers or references might point to the same person, or when one person may be represented by multiple, apparently distinct, records. In digital-identity systems this can involve cross-checking biographical attributes (date of birth, address), biometrics or behavioural signals to decide whether "Ripley" in one database is the same individual as "Rip.01" in another. Effective disambiguation prevents both mistaken merges (wrongly conflating separate

https://www.globaldata.com/store/report/digital-identity-theme-analysis/.

[561] Jesús Rivera-Guerrero et al., "Digital identity: an approach to its nature, concept, and legal implications," *International Journal of Law and Information Technology*, 2024, https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaae019/7760180.

[562] Tactical Tech, "Me and My Shadow" project, 2022. https://myshadow.org/animation.

people) and mistaken splits (treating a single person as multiple identities), thereby protecting data quality and reducing fraud risk. At scale, modern approaches combine algorithmic matching with manual review or biometric confirmation, particularly where common names or data-entry errors are rife.[563]

Disenrolment

The formal removal of an identity from a system or programme – effectively the mirror of enrolment. When a user is disenrolled, their credentials are revoked or archived; any active sessions are terminated; and associated privileges are scrubbed from access-control lists. Disenrolment may be (a) voluntary – a citizen opts out of a biometric border scheme; (b) administrative – an employer off-boards a departing staff member; or (c) sanction-based – an authority revokes an identity because of fraud or inactivity. Timely disenrolment is critical to keeping "ghost accounts" from lingering, a common vector for credential misuse.[564]

eIDAS 2.0

The 2024 revision of the EU Regulation on electronic Identification, Authentication and Trust Services. It requires Member States to offer a certified European Digital Identity Wallet for storing government-issued credentials (e.g., ID cards, driving licences) recognised across borders, with stronger privacy features such as selective disclosure. Implementation is being phased through delegated and implementing acts into 2025–26.[565]

Enrolment

The process of registering an individual into an identity system by capturing and validating evidence, establishing a new identity record, and issuing credentials bound to the person. Quality at enrolment affects downstream trust and fraud risk. [566]

Entitlement

In identity and access management, an entitlement is a specific permission or access right granted to a user. It defines what resources, data, or actions the user is allowed.

[563] U.S. Department of Homeland Security, Biometric Identity Disambiguation Technology Solution Sheet (Washington DC: DHS Science and Technology Directorate, December 2024), https://www.dhs.gov/sites/default/files/2024-12/24_1209_st_biometric_identity_disambiguation.pdf

[564] Microsoft, "Govern the Employee and Guest Lifecycle with Microsoft Entra ID Governance," Microsoft Learn (9 April 2025) https://learn.microsoft.com/en-us/entra/id-governance/scenarios/govern-the-employee-lifecycle.

[565] European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council (Brussels, 24 April 2024), EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1183/oj.

[566] United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development (Washington DC: USAID, 2017), https://www.ictworks.org/create-digital-id-inclusive-development/

Entitlements can be thought of as the fine-grained building blocks of authorization. For instance, within a system an employee might have entitlements like “Can view salary records” or “Can approve expense reports” or “Admin privileges on Database X”. These often derive from roles (like a “Manager” role might carry the entitlements to approve leave and budget) or from group memberships. Managing entitlements involves creating, auditing, and revoking these permissions as needed – a practice often called entitlement management or privilege management. It’s crucial for security that users have the correct entitlements (principle of least privilege: only what they need, no more). When a user’s job changes or they leave, their entitlements should be updated promptly (to prevent orphaned privileges). Many identity governance systems focus on tracking who has what entitlements and whether those assignments are appropriate. In summary, while “authorization” is the decision process, entitlements are the specific access rights that make up those decisions.[567]

Evil twin / Rogue AP

A malicious wireless access point set up to masquerade as a legitimate Wi-Fi network with the aim of deceiving users into connecting. An “evil twin” Wi-Fi closely mimics the name (SSID) of a genuine hotspot (like “CoffeeShop_WiFi”) in the same vicinity. Unsuspecting users connect, thinking it’s safe, but in reality they’re routing all their traffic through an attacker’s device. This allows the attacker to eavesdrop on communications, steal credentials, or perform man-in-the-middle attacks on the victim’s internet sessions. A rogue AP might also simply be an unauthorized access point plugged into a secure network by an insider, accidentally or maliciously, creating a new weak link. Both represent serious security threats. Defences include using encrypted connections (HTTPS, VPNs) so that even if one connects to a bad AP, the content remains encrypted, and being cautious about Wi-Fi networks (e.g., verifying with staff if a given hotspot is legitimate). Enterprises often use wireless intrusion detection to spot rogue APs in their environment. The term “evil twin” underscores the deceptive nature – it looks nearly identical to a trusted network, but it’s the “evil twin” that betrays you.[568]

[567] Federal Identity, Credential, and Access Management (FICAM) Program, “FICAM Architecture: Entitlement Management,” *IDManagement.gov*, 2022, https://www.idmanagement.gov/arch/.

[568] Zimperium, “Evil Twin Attacks: What They Are and How to Protect Against Them,” *Zimperium Blog*, 20 Oct 2023, https://zimperium.com/glossary/evil-twin-attacks.

Face Recognition

A biometric that identifies or verifies people from facial features. Accuracy is affected by lighting, angle, ageing, and demographic bias in models; responsible use requires PAD (liveness) and governance to mitigate surveillance harms.[569]

False Acceptance/False Rejection Rate (FAR/FRR)

Metrics used to evaluate biometric or authentication systems, representing two types of errors: *False Acceptance Rate* (FAR) is the probability that an unauthorized person is mistakenly verified as legitimate (a "false positive"), whereas *False Rejection Rate* (FRR) is the probability that a legitimate person is wrongly rejected as unauthorized (a "false negative").

In simpler terms, FAR measures how often "bad guys" get in when they shouldn't, and FRR measures how often "good guys" get blocked. For example, in a fingerprint scanner with a 1% FAR, 1 in 100 attempts by the wrong person might succeed as a match; with a 5% FRR, 1 in 20 attempts by the correct person might fail to recognize them. There's typically a trade-off between FAR and FRR, adjustable via system sensitivity or thresholds. If you make the system very strict to minimize false accepts (lower FAR), it usually increases inconvenience by causing more false rejects (higher FRR), and vice versa.

The equal error rate (EER) is a point where FAR and FRR are equal, often used as a single metric of system accuracy. In designing security, one chooses acceptable rates based on context – e.g., a high-security environment tolerates some false rejections to drive false accepts extremely low, whereas a consumer phone unlock might err on the side of usability (low FRR) while accepting a slightly higher FAR. Monitoring these rates in operation is also vital for detecting performance issues or needed recalibration in biometric systems.[570]

Federation

A trust arrangement where multiple distinct organisations recognise and accept each other's authenticated users, enabling single sign-on across organisational boundaries. One domain (the Identity Provider, IdP) authenticates the user and passes an assertion to another domain (the Service Provider, SP) that trusts the IdP, which then grants access without requiring separate login. For example, if your university and an online library have a federation agreement, you can log into the library using your university credentials – the

[569] Charles H. Romine, "Facial Recognition Technology: Examining Its Current Use, Future Prospects, and Social and Ethical Implications," testimony before the U.S. House of Representatives, *National Institute of Standards and Technology,* 26 June 2019, https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.

[570] Microblink, "Biometrics: Accuracy, FAR, and FRR," *Microblink Blog,* 2023, https://microblink.com/resources/blog/false-rejection-rate/.

library trusts the university's authentication process. Federation uses protocols such as SAML (Security Assertion Markup Language) and OAuth2/OIDC. The organisations participating in a specific federation are sometimes called a 'circle of trust' and typically adhere to common standards such as the InCommon federation for U.S. universities.[571]

Federated Identity

An identity that is portable across multiple systems or organisations thanks to federation agreements. When you have a federated identity, one account (with a particular Identity Provider) can be used to access services at various other providers without creating new accounts at each. For instance, your federated identity might be your company login, which you then use to access third-party business applications that are federated with your company. The user consents (often via a 'use this account to log in' prompt) and identity information is shared via secure tokens. Federated identity reduces the proliferation of credentials and gives the home identity provider more control and visibility for centrally enforced security policies. Classic consumer examples include using an Apple ID or Facebook ID to log into other applications.[572]

Financialisation

The process by which an activity or thing is transformed into a financial asset or its value is understood in financial terms. In digital identity or personal data contexts, financialisation means treating identity attributes and personal information as commodities with monetary value, integrating identity systems into financial markets and instruments. For example, data about individuals (purchase habits, credit scores, social media behaviour) gets packaged and traded by companies – personal data becomes a financial asset class. This highlights that beyond their practical function, identities and related services generate profits, attract investment, and are subjected to market dynamics, raising ethical questions about exploiting people's identities for profit.[573]

Fingerprint

The unique pattern of ridges and whorls on a person's fingertip, commonly used as a biometric identifier. No two individuals (even identical twins) have exactly the same fingerprint patterns. In digital identity systems, a fingerprint refers either to the physical

[571] Gerald Epstein, "Financialization: What It Is and Why It Matters," IMK Working Paper, Political Economy Research Institute, University of Massachusetts at Amherst, 2005, https://www.peri.umass.edu/publication/item/153-financialization-what-it-is-and-why-it-matters.

[572] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

[573] Greta R. Krippner, 'The Financialization of the American Economy,' *Socio-Economic Review* 3, no. 2 (2005): 173-208, https://doi.org/10.1093/SER/mwi008.

biometric itself or to the digital template representation of it. During enrollment, a scanner captures the fingerprint image and extracts key features (minutiae points like ridge endings and bifurcations). Later, during verification, a new scan is compared to the stored template to determine if they match above a certain threshold. Fingerprint recognition is popular in consumer devices and access control due to its balance of convenience and uniqueness, though it has limitations with dirty or injured fingers and non-zero false match rates.[574]

First Principle

A basic, fundamental truth or assumption that serves as a foundation for reasoning. In problem-solving and system design, 'thinking from first principles' means breaking a concept down to its core elements and reasoning up anew, instead of relying on analogy or status quo. For example, in identity systems, a first principle might be that 'identity is the link between a subject and attributes' – starting from that, one could derive how systems should verify and maintain that link. The concept originates from philosophy and mathematics, where first principles are axioms that cannot be derived from anything else. First principles thinking prevents reliance on assumptions and ensures each design decision stands on solid logical ground.[575]

Foundational ID System

A government-backed identification system designed to provide universal, official identity to the general population, usable across many sectors of society. Examples include national ID card programmes, population registries, or civil registration systems. Foundational IDs establish legal identity in the eyes of the law and often come with a unique identifier (like a national ID number). They are called 'foundational' because they serve as the base for other functional identities – your national ID might be needed to get a driver's licence, passport, or open a bank account. Such systems aim for widespread coverage (ideally every citizen and resident) and are used for public administration, voting, and social services, with a key aspect being uniqueness to prevent one person from having multiple identities.[576]

GDPR Data-Subject Rights

The rights granted to individuals under the EU General Data Protection Regulation to maintain control and transparency over their personal data. Key GDPR data-subject

[574] Wencheng Yang et al., 'Security and Accuracy of Fingerprint-Based Biometrics: A Review,' *Symmetry* 11, no. 2 (2019): 141, https://doi.org/10.3390/sym11020141.

[575] Norman L. Geisler, "The First Principles of Knowledge," *CTS Journal* 3, no. 3, 1997, https://normangeisler.com/the-first-principles-of-knowledge/.

[576] World Bank Group, 'Types of ID Systems,' Identification for Development (ID4D) Initiative, accessed 10 December 2024, https://id4d.worldbank.org/guide/types-id-systems.

rights include: Right to be Informed (organisations must disclose what data they collect and why), Right of Access (individuals can request copies of their data), Right to Rectification (correct inaccurate data), Right to Erasure (right to be forgotten), Right to Restrict Processing (limit how organisations use data), Right to Data Portability (receive data in portable formats), Right to Object (to certain processing like direct marketing), and rights concerning automated decision-making and profiling (protection against solely algorithmic decisions with legal significance). These rights emphasise transparency, empowerment, and accountability in personal data handling, requiring organisations to implement processes to handle requests typically within one month.[577]

Gait

An individual's manner of walking used as a behavioural biometric identifier. Gait analysis examines unique patterns in a person's walk – stride length, limb movement, posture, and rhythm – which are largely subconscious and difficult to mimic precisely. This enables authentication at a distance without subject cooperation, making it valuable for CCTV security systems, forensic identification, and continuous authentication (such as smartphones using accelerometer data). Environmental factors including footwear, terrain, and injuries can affect gait patterns, limiting accuracy compared to physiological biometrics. While less widely deployed than fingerprints or facial recognition due to these complexities, gait recognition offers the advantage of unobtrusive capture and difficulty of impersonation.[578]

Hardware Security Module (HSM)

A tamper-resistant physical computing device dedicated to securely managing cryptographic keys and operations. HSMs act as trust anchors by protecting cryptographic material within hardened, tamper-evident devices that resist physical interference attempts. They perform cryptographic functions – encryption, decryption, digital signing – inside their protected environment, ensuring keys never leave the secure boundary. HSMs are used for high-security applications including protecting certification authority private keys, banking transaction signing, cryptocurrency exchange security, and DNS root keys. They provide secure key generation using true random number generators, hardware-based

[577] Regulation [EU] 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [General Data Protection Regulation], OJ 2016 L 119/1, https://gdpr-info.eu/.

[578] Patrick Connor and Arun Ross, 'Biometric Recognition by Gait: A Survey of Modalities and Features,' *Computer Vision and Image Understanding* 167 [2018]: 1–27, https://doi.org/10.1016/j.cviu.2017.09.007.

performance optimization, and protection against both remote and physical attacks. Most HSMs are certified to FIPS 140-3 or Common Criteria standards.[579]

Hardware Token

A physical device used for authentication, providing evidence of 'something you have' in multi-factor authentication systems. Hardware tokens include key fobs displaying changing codes, smart cards with embedded chips, USB tokens, and wireless devices. They generate one-time passwords (OTPs) or time-based one-time passwords (TOTPs) that users input during authentication, or perform cryptographic operations to sign challenges from authentication systems. Modern hardware tokens like FIDO2/WebAuthn security keys use public-key cryptography to resist phishing attacks. Hardware tokens significantly enhance security as remote attackers cannot duplicate them digitally – physical possession is required. While they offer strong security, drawbacks include potential loss, replacement logistics, and user inconvenience of carrying an additional device.[580]

Holder

In digital identity frameworks, particularly self-sovereign identity (SSI), the entity (person or organisation) that possesses and controls identity credentials. In the issuer-holder-verifier triangle, the holder receives credentials from issuers, stores them (typically in a digital wallet), and presents them to verifiers when authentication is required. The holder maintains autonomy over their credentials, deciding when and with whom to share specific information or claims. This concept emphasises user control and data sovereignty, contrasting with centralised models where third parties manage identity data. In SSI systems, holders can generate decentralised identifiers (DIDs) and use selective disclosure to share only necessary information, maintaining privacy while enabling verification.[581]

Identity

In digital contexts, the set of attributes or references that uniquely describe an entity within a given system or context. Digital identity encompasses any data that distinguishes one entity from others – names, identifiers, credentials, biometric data, and authentication factors. Individuals typically maintain multiple digital identities across different services, each tailored to specific contexts and requirements. Identity enables authentication (verifying *who you are*) and authorisation (determining *what you can*

[579] National Institute of Standards and Technology, 'Hardware Security Module (HSM),' *Computer Security Resource Center*, accessed 2 April 2025, https://csrc.nist.gov/glossary/term/hardware_security_module_hsm.

[580] Kason Andress, 'Chapter 2 - Identification and Authentication,' in The Basics of Information Security, *ScienceDirect*, 2011, https://www.sciencedirect.com/science/article/abs/pii/B9781597496537000025.

[581] Christopher Allen, 'Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy,' *PMC*, 28 July 2022, https://pmc.ncbi.nlm.nih.gov/articles/PMC9371034/.

access). The identity lifecycle involves establishment through identity proofing, ongoing management and updates, and eventual deactivation. Legal identity (recognised by governmental authorities) differs from digital identity (broader online representation), though they increasingly intersect in digital government services and credentialing systems.[582]

Identity collapse

A phenomenon whereby multiple distinct facets of an individual's digital identity converge into a single context, potentially compromising privacy boundaries and contextual integrity. This convergence occurs when separate identity domains – professional, personal, social, or anonymous – become inadvertently merged through technological architectures or platform design decisions. The concept encompasses both spatial collapse, where diverse audiences converge around single communicative acts, and temporal collapse, where historical digital traces become accessible across time boundaries. Identity collapse manifests technically when identifiers intended for discrete contexts become linked, such as when pseudonymous accounts are connected to verified identities. The phenomenon highlights fundamental tensions between usability and privacy in digital identity systems, often resulting in self-censorship behaviours and reduced authentic self-expression as users attempt to manage multiple audience expectations simultaneously.[583]

Identity Graph

A data structure that maps and interconnects all digital identifiers and attributes associated with an individual across multiple systems, platforms, and interaction contexts. Utilising graph theory principles, these models position individuals as central nodes connected through edges representing relationships between various identifiers – including email addresses, device identifiers, cookies, mobile advertising IDs, and behavioural metadata. Identity graphs employ both deterministic matching (exact identifier correlation) and probabilistic matching (pattern-based likelihood algorithms) to establish entity relationships. In commercial applications, these structures enable unified customer experience delivery and cross-device attribution, whilst in security contexts they facilitate fraud detection through suspicious account correlation. The construction and maintenance of identity graphs raises significant privacy considerations, as they inherently enable de-

[582] International Organization for Standardization, ISO/IEC 24760-1:2019, 'IT Security and Privacy—A Framework for Identity Management—Part 1: Terminology and Concepts,' 2011, https://www.iso.org/standard/57914.html.

[583] Alice Marwick and danah boyd, "I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience," *New Media & Society* 13, no. 1 (2011): 114-133, https://journals.sagepub.com/doi/10.1177/1461444810365313.

anonymisation across platforms and require careful attention to data protection compliance frameworks.[584]

Identity Lifecycle Management

The comprehensive process encompassing the creation, maintenance, modification, and termination of digital identities within organisational information systems. This methodology addresses three primary phases: provisioning (identity creation and initial access rights assignment), maintenance (ongoing attribute updates, role modifications, and access right adjustments), and deprovisioning (account disabling and data archival upon user departure). Modern identity lifecycle management integrates with human resources systems to automate joiner-mover-leaver workflows, ensuring temporal alignment between employment status and digital access rights. Advanced implementations incorporate Identity Governance and Administration (IGA) platforms that enforce least privilege principles through automated role-based access control and periodic access certification processes. Effective lifecycle management reduces security vulnerabilities associated with orphaned accounts whilst improving operational efficiency through standardised identity management procedures.[585]

Identity Orchestration

The dynamic coordination and integration of multiple identity-related services and processes to deliver contextually appropriate authentication and authorisation experiences. This architectural approach enables real-time decision-making by orchestrating various identity components – including directory services, risk assessment engines, multi-factor authentication systems, and fraud detection mechanisms – based on situational risk profiles and user context. Identity orchestration platforms utilise policy engines and workflow automation to adapt authentication requirements dynamically, implementing principles such as step-up authentication for high-risk transactions or streamlined access for trusted contexts. Modern implementations support visual policy builders enabling non-technical administrators to configure complex authentication flows without extensive programming knowledge. This approach proves essential for implementing Zero Trust architectures and managing customer identity journeys across diverse digital touchpoints whilst maintaining security efficacy and user experience optimisation.[586]

[584] "How Identity Graphs Are Built—Present and Future," The Trade Desk, 6 March 2024, https://www.thetradedesk.com/resources/how-identity-graphs-are-built-the-present-and-the-future.

[585] "What Is IGA [Identity Governance & Administration]?," *One Identity*, accessed 7 January 2025, https://www.oneidentity.com/what-is-iga/.

[586] "Leadership Compass: Customer Identity and Access Management [CIAM]," *KuppingerCole*, 3 June 2024, https://www.kuppingercole.com/research/lc80834/customer-identity-and-access-management-ciam.

Identity Portability

The capability for individuals to transfer and utilise their digital identity credentials across different platforms, services, and identity providers with minimal friction or vendor lock-in. This concept encompasses both technical interoperability – through standards such as OAuth, OpenID Connect, and SAML – and user empowerment through self-sovereign identity models that enable credential reuse across service boundaries. Identity portability addresses both regulatory requirements, such as the GDPR's data portability provisions, and user experience considerations by reducing repetitive onboarding processes and enabling competitive service switching. Advanced implementations leverage verifiable credentials and decentralised identifier technologies to enable portable digital attestations that users can present to any service without requiring re-verification. True identity portability requires robust trust frameworks to ensure cross-platform credential acceptance whilst maintaining security and privacy protections.[587]

Identity Proofing

The systematic process of verifying and validating that an individual is who they claim to be in the physical world prior to establishing their digital identity credentials. This process involves three distinct phases: resolution (establishing uniqueness within a given population), validation (confirming the authenticity and accuracy of presented evidence), and verification (binding the validated evidence to the actual person). Identity proofing methodologies are categorised by Identity Assurance Levels (IAL), ranging from self-assertion (IAL1) to supervised physical presence with biometric verification (IAL3). Advanced implementations utilise automated document verification technologies, biometric comparison systems, and knowledge-based verification processes to establish confidence in claimed identities. The strength of identity proofing directly impacts the trustworthiness of subsequent digital interactions and determines the appropriate level of access or privileges that can be safely granted to verified individuals.[588]

Identity Provider (IdP)

A system entity that creates, maintains, and manages digital identity information for users whilst providing authentication services to relying party applications within federated environments. Identity providers serve as trusted authorities that validate user credentials and issue security assertions – typically through SAML, OAuth, or OpenID

[587] Christopher Allen, “Self-Sovereign Identity Principle #6: Portability,” *Metadium*, 8 December 2021, https://medium.com/metadium/self-sovereign-identity-principle-6-portability-4a7105dd0381.

[588] Paul A. Grassi et al., “NIST Special Publication 800-63A: Digital Identity Guidelines—Enrollment and Identity Proofing,” *National Institute of Standards and Technology*, June 2017, doi:10.6028/NIST.SP.800-63a, https://pages.nist.gov/800-63-3/sp800-63a.html.

Connect protocols – enabling single sign-on capabilities across multiple service providers. Modern identity providers extend beyond simple credential storage to offer comprehensive identity services including multi-factor authentication, risk-based access control, and user attribute management. In federated architectures, identity providers establish trust relationships with service providers through metadata exchange and certificate-based security, enabling secure cross-domain authentication without requiring users to maintain separate credentials for each service. The selection and configuration of identity providers significantly impacts both security posture and user experience within organisational digital ecosystems.[589]

Identity Resolution

The systematic process of determining that disparate identifiers, accounts, or data records from multiple sources refer to the same individual or entity, thereby enabling unified profile creation across heterogeneous information systems. This analytical methodology employs both deterministic matching – utilising exact correspondences between unique identifiers such as email addresses or government-issued numbers – and probabilistic matching – leveraging algorithmic inference to establish connections based on behavioural patterns, device characteristics, and contextual similarities. Identity resolution techniques facilitate comprehensive customer relationship management by linking web cookies, mobile application interactions, and offline purchase records into coherent identity graphs. Advanced implementations incorporate machine learning algorithms to assess match confidence scores and manage complex scenarios involving data inconsistencies or incomplete information. The process proves essential for fraud detection, where suspicious account relationships become apparent through cross-system correlation, and for regulatory compliance requiring unified customer views across organisational boundaries.[590]

ID Scheme / ID System / ID Ecosystem

A hierarchical taxonomy describing digital identity architecture across three interrelated layers of complexity and governance scope. An ID scheme constitutes the foundational technology stack, encompassing specific protocols, data structures, and cryptographic implementations that enable identity verification and credential management. An ID system extends this technical foundation by incorporating governance frameworks, policy constraints, and operational procedures that regulate scheme

[589] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

[590] "Deterministic vs. Probabilistic Matching," *GrowthLoop University*, 19 March 2024, https://www.growthloop.com/university/article/deterministic-vs-probabilistic-matching.

deployment within defined organisational or jurisdictional boundaries. An ID ecosystem represents the broader federated environment where multiple systems interact, often with overlapping authorities, competing standards, and complex interoperability requirements that generate both synergies and conflicts between participating entities. These architectural layers reflect increasing complexity in trust relationships, from technical protocol adherence at the scheme level to multi-stakeholder governance at the ecosystem level. Understanding this taxonomy proves crucial for designing interoperable identity solutions that can operate effectively across organisational boundaries whilst maintaining security and privacy requirements.[591]

Identity Theft

Unauthorised acquisition and use of someone's personally identifiable information for fraud or other crimes. Techniques range from document theft and phishing to data breaches and malware; synthetic identity fraud blends real and fabricated data. Mitigation requires stronger authentication, reduced reliance on static identifiers, and rapid detection and recovery processes.[592]

Identity Wallet

A user-controlled digital application designed for secure storage, management, and selective presentation of verifiable credentials and identity attestations. Operating as the digital equivalent of physical wallets, these applications enable individuals to maintain custody of their identity documents (including educational certificates, professional licenses, government-issued identifications, and access credentials) whilst exercising granular control over data sharing decisions. Modern identity wallets implement cryptographic protection mechanisms, typically secured through biometric authentication or PIN verification, and support privacy-preserving presentation techniques including zero-knowledge proofs that enable attribute verification without revealing underlying personal data. The European Union's eIDAS 2.0 framework mandates that Member States provide digital identity wallets to all citizens by 2026, representing a significant advancement toward user-centric identity management. These applications embody self-sovereign identity principles by positioning individuals as the authoritative controllers of

[591] European Parliament and Council, *Regulation (EU) 2024/2844 of the European Parliament and of the Council of 13 March 2024 on a framework for a European digital identity* (eIDAS 2.0), OJ L 2024/2844 (13 March 2024), art. 3(6), https://www.european-digital-identity-regulation.com/Article_3_(Regulation_EU_2024_1183).html.

[592] U.S. Department of Justice, "Identity Theft and Identity Fraud," *justice.gov* (last updated 28 June 2023), https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

their digital identity ecosystem, fundamentally shifting from traditional models where identity data remains distributed across multiple service provider databases.[593]

Identifier

A discrete data element that uniquely distinguishes a specific entity – individual, device, account, or digital asset – within a defined contextual scope or namespace. Digital identifiers range from human-readable formats such as usernames and email addresses to machine-optimised constructs including Universally Unique Identifiers (UUIDs), cryptographic hashes, and decentralised identifiers (DIDs). Identifier design considerations encompass scope limitations (global versus local uniqueness), persistence requirements (temporal stability versus ephemeral usage), and privacy implications inherent in their structure and deployment patterns. Contemporary identity architectures often require multiple identifiers per entity to support different functional contexts – authentication, authorisation, audit trails, and cross-system correlation – whilst maintaining appropriate privacy boundaries. Effective identifier management proves fundamental to digital identity systems, as these elements serve as the primary mechanism for entity reference and relationship establishment across complex, distributed computing environments where traditional contextual cues remain unavailable.[594]

Identification

The process of establishing or determining an entity's identity within a system through the presentation or recognition of distinguishing attributes. Identification encompasses both active credential presentation (usernames, identity documents, biometric samples) and passive system recognition (device fingerprinting, environmental detection). This foundational step precedes authentication and establishes the identity claim that subsequent verification processes validate. In access control frameworks, identification creates the initial identity assertion upon which authentication mechanisms operate.[595]

Identification Collapse

A critical failure condition in identity management systems where the infrastructure loses its capacity to reliably distinguish between distinct entities. This phenomenon manifests through erroneous identity consolidation, irreconcilable data

[593] "European Digital Identity," European Commission, accessed 19 December 2024, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

[594] Lasse Nitz et al., "Evaluation of Unique Identifiers Used as Keys to Match Identical Publications in Pure and SciVal–A Case Study from Health Science," *PLOS ONE* 11, no. 9 (2016), doi:10.1371/journal.pone.0162894, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5017295/.

[595] Okta, "Identification and Authentication: Similarities and Differences," *Okta Identity 101*, updated 27 August 2024, https://www.okta.com/identity-101/identification-vs-authentication/.

conflicts preventing accurate resolution, or systematic misidentification affecting multiple subjects simultaneously. Such failures undermine fundamental security assumptions and may precipitate unauthorised access, data attribution errors, and cascading trust failures across interconnected systems. Common precipitating factors include biometric sensor degradation, database schema incompatibilities, or deliberate poisoning attacks targeting system integrity.[596]

Impersonation

The deliberate assumption of another entity's identity to deceive authentication systems and gain unauthorised advantages. Digital impersonation encompasses credential theft, synthetic identity creation, and sophisticated deception techniques including deepfake technologies for biometric spoofing. Successful impersonation represents authentication system failure and constitutes a primary threat vector in identity security frameworks. Contemporary defensive measures include multi-factor authentication protocols, behavioural analytics, and robust identity verification procedures during credential recovery processes.[597]

Infrastructural Approach

A strategic framework conceptualising digital identity as foundational infrastructure analogous to telecommunications or transport networks. This paradigm emphasises interoperability, scalability, and universal accessibility through standardised protocols and comprehensive governance frameworks. Infrastructural identity systems serve diverse stakeholders across multiple sectors, requiring substantial coordination and investment whilst enabling broad innovation through shared identity infrastructure. This approach contrasts with instrumental implementations that optimise for specific use cases.[598]

Instrumental Approach

A targeted design methodology creating identity systems for specific, well-defined purposes rather than broad utility. Instrumental implementations optimise for particular use cases such as welfare distribution or corporate access control, potentially resulting in

[596] Jan Camenisch and Els Van Herreweghen, 'Design and Implementation of the idemix Anonymous Credential System', *Proceedings of the 9th ACM Conference on Computer and Communications Security* (2002): 21-30, https://dl.acm.org/doi/10.1145/586110.586114.

[597] Andrea Bonissi, Ruggero Donida Labati, Vincenzo Piuri, and Fabio Scotti, 'Advances in Biometric Technologies: Challenges and Opportunities,' *IEEE Computer Society* (2019): 47-53, https://www.frontiersin.org/research-topics/62996/new-generation-of-attacks-on-biometric-user-authentication-systems.

[598] Silvia Masiero and Savita Bailur, 'Digital Identity for Development: The Quest for Justice and a Research Agenda,' *Information Technology for Development* 27, no. 3 (2021): 397-412, https://www.tandfonline.com/doi/full/10.1080/02681102.2021.1859669.

fragmented, non-interoperable identity ecosystems. Whilst efficient for immediate objectives, this approach may constrain scalability and limit cross-sector integration opportunities. The selection between instrumental and infrastructural approaches represents a fundamental strategic decision in identity system architecture.[599]

Iris

The coloured annular tissue surrounding the pupil, containing unique anatomical patterns suitable for biometric identification. Iris recognition employs specialised infrared imaging to capture detailed textural features including crypts, furrows, and striations, encoding these into digital templates for matching algorithms. The iris demonstrates exceptional biometric performance characteristics due to pattern stability throughout life, genetic uniqueness between individuals (including identical twins), and natural protection from environmental degradation. Contemporary iris systems incorporate sophisticated liveness detection mechanisms to counter presentation attacks.[600]

Issuance

The formal process of creating and delivering identity credentials to verified subjects following successful identity proofing procedures. Issuance encompasses credential personalisation, secure delivery mechanisms, and establishment of the cryptographic or procedural trust relationship between issuer and credential holder. This critical juncture determines credential integrity and requires comprehensive security controls to prevent unauthorised credential generation or interception during distribution. Post-issuance responsibilities include credential lifecycle management, renewal procedures, and revocation capabilities.[601]

Issuer

An authoritative entity responsible for creating, digitally signing, and distributing identity credentials or attestations within trust frameworks. Issuers function as trust anchors in identity ecosystems, with their credibility and security practices determining credential trustworthiness and acceptance by relying parties. Examples include governmental agencies issuing passports, educational institutions granting diplomas, and certification authorities providing digital certificates. Issuer compromise represents

[599] Alexandra Giannopoulou, 'Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity,' *Digital Society* 2, no. 14 (2023): 1-23, https://link.springer.com/article/10.1007/s44206-023-00049-z.

[600] Alaa S. Al-Waisy, Rami Qahwaji, Stanley Ipson, Shumoos Al-Fahdawi, and Tarek A.M. Nagem, 'A Multi-Biometric Iris Recognition System Based on a Deep Learning Approach,' *Pattern Analysis and Applications* 21, no. 3 (2018): 783-802, https://link.springer.com/article/10.1007/s10044-017-0656-1.

[601] World Bank Group, 'Credential Issuing,' *Identification for Development* (2024), https://id4d.worldbank.org/guide/credential-issuing.

significant systemic risk, necessitating robust key management practices and comprehensive governance frameworks.[602]

Passive Biometry

Biometric identification conducted without subject awareness, knowledge, or explicit consent, typically through ambient surveillance infrastructure. Also termed covert or surveillance biometry, this capability enables identification through environmental sensors including facial recognition cameras, ambient voice analysis, or gait detection systems without active subject participation. Whilst offering operational advantages in security applications, passive biometry raises substantial privacy, consent, and civil liberties concerns requiring careful ethical and legal consideration in deployment contexts.[603]

Passkey

A phishing-resistant, WebAuthn/FIDO2 public-key credential. The private key stays on the user's device (e.g., in a secure enclave); the service holds only the public key. Users unlock the credential with a local biometric or PIN; some ecosystems offer encrypted multi-device sync/backup.[604]

Password / Passphrase

Knowledge-based authentication credentials comprising memorised secrets for identity verification. Passwords typically consist of character strings with specified complexity requirements, whilst passphrases employ longer, more memorable word sequences providing enhanced entropy through length rather than complexity. Both function as 'something you know' authentication factors but suffer from fundamental security limitations including susceptibility to credential stuffing, social engineering, and reuse across multiple systems. Contemporary security frameworks increasingly favour multi-factor authentication or passwordless alternatives to address these inherent vulnerabilities.[605]

[602] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello, 'Decentralized Identifiers (DIDs) v1.0', *W3C Recommendation* (2022), https://www.w3.org/TR/did-core/.

[603] Privacy Commissioner of Canada, 'Data at Your Fingertips: Biometrics and the Challenges to Privacy,' *Office of the Privacy Commissioner of Canada* (2011), https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/.

[604] Passkey Central, "How Passkeys Work," *Passkey Central*, https://www.passkeycentral.org/introduction-to-passkeys/how-passkeys-work.

[605] Dinei Florêncio, Cormac Herley, and Paul C. van Oorschot, 'Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts,' *Proceedings of the 23rd USENIX Security Symposium* (2014): 575–590, https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/florencio.

Person-Bound Credential

An identity credential cryptographically or procedurally bound to a specific individual, designed to prevent transfer, sharing, or unauthorised usage by other parties. Person-binding mechanisms include biometric templates embedded within credentials, hardware security modules tied to individual characteristics, or cryptographic key pairs where private keys cannot be extracted or shared. This binding ensures credential non-transferability and enhances authentication assurance by creating strong linkage between the credential holder and the authenticated identity.[606]

Performative Identity

A conceptual framework understanding identity as an ongoing, contextual enactment rather than a fixed, essential characteristic. Drawing from Judith Butler's theories of performativity, this approach recognises identity as constituted through repeated acts and performances within social and technological contexts. In digital environments, performative identity manifests through profile curation, platform-specific self-presentation, and algorithmic interactions that continuously reconstitute identity through technological mediation. This perspective challenges essentialist identity models by emphasising the dynamic, contextual nature of identity construction.[607]

Phishing

A social engineering attack methodology employing deceptive communications to manipulate recipients into divulging sensitive information or executing malicious actions. Phishing attacks exploit human psychological vulnerabilities through urgency, authority impersonation, and trust manipulation rather than technical system vulnerabilities. Contemporary variants include spear phishing (targeted attacks), whaling (executive-focused attacks), and sophisticated multi-vector campaigns combining email, voice, and social media channels. Effective countermeasures require both technological solutions and comprehensive user education programmes addressing human factors in cybersecurity.[608]

Poisoned Model

A compromised machine learning model deliberately corrupted through malicious training data injection or algorithmic manipulation. In biometric systems, poisoned models

[606] Rachna Dhamija, and Lisa Dusseault, 'The Seven Flaws of Identity Management: Usability and Security Challenges,' *IEEE Security & Privacy* 6, no. 2 (2008): 24-29, https://ieeexplore.ieee.org/document/4494647.

[607] Judith Butler, 'Performative Acts and Gender Constitution: An Essay in Phenomenology and Feminist Theory,' *Theatre Journal* 40, no. 4 (1988): 519-531, https://www.jstor.org/stable/3207893.

[608] Elmer Lastdrager, Ira Carvajal Gallardo, Prokopis Hartel, and Marianne Junger, 'How Effective is Anti-Phishing Training for Children?', *Proceedings of the 13th Symposium on Usable Privacy and Security* (2017): 229-239, https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager.

may produce false acceptances for specific adversarial inputs whilst maintaining normal performance on legitimate data. Model poisoning represents a sophisticated attack vector targeting the integrity of learning algorithms rather than traditional security perimeters. Defences include robust training methodologies, data provenance verification, and model behaviour monitoring to detect algorithmic manipulation.[609]

Policy

Formal governance frameworks establishing rules, procedures, and constraints governing identity system operation and user behaviour. Policies encompass technical specifications (authentication requirements, data handling procedures), organisational directives (access control matrices, incident response protocols), and compliance mandates (regulatory adherence, audit requirements). Effective policy frameworks balance security objectives with usability requirements whilst ensuring legal compliance and stakeholder accountability throughout identity system lifecycles.[610]

Presentation Attack

An attack on a biometric system using artefacts (printed face, silicone fingerprint, synthetic voice) to impersonate a subject. Presentation Attack Detection (PAD) includes liveness checks, challenge/response, and multi-modal verification (see ISO/IEC 30107).[611]

Privileged Access Management (PAM)

A cybersecurity discipline encompassing strategies, technologies, and processes for controlling, monitoring, and auditing elevated access rights within organisational IT environments. PAM implements least-privilege principles through just-in-time access provisioning, credential vaulting, session recording, and privilege analytics. This framework addresses the disproportionate risk associated with administrative accounts that possess extensive system permissions, representing high-value targets for adversaries and insider threats. Modern PAM solutions integrate with Zero Trust architectures and provide comprehensive audit trails for compliance requirements.[612]

[609] Battista Biggio, and Fabio Roli, ‘Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning,’ *Pattern Recognition* 84 (2018): 317-331, https://www.sciencedirect.com/science/article/pii/S0031320318302565.

[610] Ross Anderson, ‘Security Engineering: A Guide to Building Dependable Distributed Systems,’ 3rd ed. (Indianapolis: Wiley, 2020), Chapter 4, https://www.cl.cam.ac.uk/~rja14/book.html.

[611] Sébastien Marcel, Mark S. Nixon, Julian Fierrez, and Nicholas Evans, eds., *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*, 3rd ed. (Singapore: Springer, 2023), https://link.springer.com/book/10.1007/978-981-19-5288-3.

[612] Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne, *Operating System Concepts*, 10th ed. (Hoboken: Wiley, 2018), Chapter 17, https://www.os-book.com/OS10/.

Profile

A structured collection of identity attributes, preferences, and behavioural data representing an individual within a digital system or platform. Profiles aggregate diverse data types including demographic information, service usage patterns, social connections, and preference settings to enable personalised system interactions. In federated identity systems, profiles may distribute across multiple authorities whilst maintaining coherent identity representation through standardised attribute schemas and secure synchronisation mechanisms. Profile management encompasses privacy controls, attribute lifecycle management, and consent frameworks.[613]

Programmable Personhood

An emerging concept describing algorithmic determination of individual rights, privileges, and social standing through automated assessment of digital behavioural patterns and data profiles. This paradigm represents the convergence of artificial intelligence, digital identity, and governance systems to create dynamic, contextual definitions of citizenship and social participation. Programmable personhood raises fundamental questions about human agency, algorithmic bias, and the delegation of social classification to automated systems.[614]

Proof of Personhood

Verification mechanisms establishing that a digital identity corresponds to a unique, living human individual rather than an automated system, duplicate account, or synthetic identity. Proof of personhood protocols address the challenge of ensuring ‘one person, one account’ principles in digital systems vulnerable to Sybil attacks and automated abuse. Implementation approaches include biometric verification, social graph analysis, stake-based systems, and cryptographic protocols enabling privacy-preserving uniqueness verification without revealing personal information.[615]

Public/Private Key Pair

A cryptographic construct comprising two mathematically related keys enabling asymmetric encryption and digital signature operations. The public key, freely distributable, enables encryption and signature verification, whilst the private key,

[613] Dick Hardt, ed., ‘The OAuth 2.0 Authorization Framework,’ *RFC 6749* [2012], https://tools.ietf.org/html/rfc6749.

[614] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* [New York: PublicAffairs, 2019], https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/.

[615] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford, ‘Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies,’ *Proceedings of the IEEE European Symposium on Security and Privacy Workshops* [2017]: 23–26, https://ieeexplore.ieee.org/document/7966966.

maintained in strict secrecy, enables decryption and signature generation. This asymmetric relationship resolves key distribution challenges inherent in symmetric cryptography by eliminating the need for shared secrets. Key pairs form the foundation of public key infrastructure, enabling secure communications, authentication, and non-repudiation in distributed systems.[616]

Public-Key Infrastructure (PKI)

A comprehensive framework encompassing policies, procedures, hardware, software, and standards required to manage digital certificates and public-key cryptography deployment. PKI facilitates secure electronic transactions through certificate authorities that issue, validate, and revoke digital certificates binding public keys to verified identities. This infrastructure enables encryption, digital signatures, and authentication across distributed networks whilst providing scalable key management for large organisations. PKI implementations require careful consideration of trust models, certificate lifecycle management, and revocation mechanisms to maintain security and operational effectiveness.[617]

Pseudonymity / Pseudonymous Identifier

The use of persistent but non-directly-identifying labels that enable consistent interaction whilst obscuring real-world identity linkages. Pseudonymous systems allow individuals to build reputation and maintain relationships under consistent identifiers without revealing personal information. This approach balances privacy protection with accountability by enabling traceability through authorised parties whilst preventing casual surveillance and correlation. Effective pseudonymous systems require robust identity separation, protection against linkage attacks, and carefully designed revelation protocols for legitimate investigative purposes.[618]

Re-Binding

The procedural framework for establishing new cryptographic associations between authenticators and subscriber accounts within identity management systems. Re-binding occurs when additional authenticators are associated with existing subscriber identities,

[616] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography* (Boca Raton: CRC Press, 1996), https://cacr.uwaterloo.ca/hac/.

[617] Russell Housley, Warwick Ford, Tim Polk, and David Solo, *‘Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*,’ RFC 5280 (2008), https://tools.ietf.org/html/rfc5280.

[618] Andreas Pfitzmann and Marit Hansen, ‘A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,’ *Technical Report TUD-FI10-01* (2010), https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

typically requiring multi-factor authentication or equivalent security measures to ensure the binding protocol maintains security commensurate with the target assurance level.[619]

Re-Key

The systematic process of generating and deploying new cryptographic keys to replace existing keys within a cryptographic system, typically performed to maintain operational security when key compromise is suspected or as part of routine key lifecycle management protocols. Re-keying operations must ensure continuity of cryptographic services whilst establishing fresh cryptographic material.[620]

Re-Proofing

The requirement for subscribers to repeat identity verification processes when they have lost all authenticators necessary to complete multi-factor authentication. Re-proofing typically involves reconfirming the binding between the claimant and previously-supplied identity evidence, with the rigour of verification procedures scaled according to the identity assurance level requirements and risk assessment outcomes.[621]

Recovery

The restoration of access to digital systems, accounts, or cryptographic materials following loss, compromise, or unavailability of primary authentication mechanisms. Recovery processes encompass both technical procedures for regaining system access and administrative workflows for validating identity claims during restoration operations.[622]

Recovery Kit / Seed Phrase

A human-readable sequence of 12–24 mnemonic words that cryptographically represents the master seed for hierarchical deterministic cryptocurrency wallets, conforming to the BIP39 standard. The seed phrase enables complete wallet recovery and private key regeneration across compatible implementations, serving as the ultimate backup mechanism for securing digital asset access whilst maintaining usability through natural language encoding.[623]

[619] National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, SP 800-63B [rev. 3 draft] [August 2023], https://pages.nist.gov/800-63-3/sp800-63b.html.

[620] National Institute of Standards and Technology, "Re-Key," Computer Security Resource Center [CSRC] Glossary [n.d.], https://csrc.nist.gov/glossary/term/re_key_certificate.

[621] National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, SP 800-63B [rev. 3 draft] [August 2023], https://pages.nist.gov/800-63-3/sp800-63b.html.

[622] National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, SP 800-63B [rev. 3 draft] [August 2023], https://pages.nist.gov/800-63-3/sp800-63b.html.

[623] National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, SP 800-63B [rev. 3 draft] [August 2023], https://pages.nist.gov/800-63-3/sp800-63b.html.

Relying Party (RP)

An entity that depends upon the validity and authenticity of subscriber credentials or identity assertions to make access control decisions, process transactions, or provide services. Within federated identity architectures, relying parties consume authentication assertions from identity providers, implementing verification protocols to establish confidence in presented identity claims before granting access to protected resources.[624]

Replay Attack

A network security exploit wherein valid data transmissions are maliciously captured and subsequently retransmitted to deceive receiving systems into accepting fraudulent communications as legitimate. Replay attacks leverage the interception and re-presentation of authentic authentication credentials or transaction data, exploiting temporal vulnerabilities in protocols that lack adequate freshness mechanisms or anti-replay protections.[625]

Residual Data

Information remnants that persist on storage media after standard deletion or formatting operations, potentially containing sensitive data that remains recoverable through forensic analysis techniques. Residual data represents a critical security consideration in media sanitisation, as conventional data removal methods may leave exploitable information traces accessible to unauthorised parties with sufficient technical capabilities.[626]

Retina

The neural tissue layer at the posterior aspect of the human eye, characterised by unique vascular patterns that serve as highly distinctive biometric identifiers for authentication systems. Retinal scanning technology employs low-intensity infrared illumination to capture the intricate blood vessel architecture, providing one of the most accurate biometric modalities with extremely low false acceptance and rejection rates, particularly suitable for high-security applications.[627]

[624] Mozilla Developer Network (MDN), "Relying Party," *MDN Web Docs* (n.d.), https://developer.mozilla.org/en-US/docs/Glossary/Relying_party.

[625] National Institute of Standards and Technology, "Replay Attack," *CSRC Glossary* (n.d.), https://csrc.nist.gov/glossary/term/replay_attack.

[626] Andrew R. Regenscheid, Larry Feldman, and Gregory A. Witte, "NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization," *National Institute of Standards and Technology*, 5 February 2015, https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization.

[627]

Revocation

The formal process of permanently invalidating the binding between a digital certificate and its associated identity before the certificate's natural expiration date. Revocation renders certificates untrustworthy and unusable for cryptographic operations, typically implemented through certificate revocation lists (CRLs) or online certificate status protocol (OCSP) mechanisms to prevent continued reliance on compromised or invalid credentials.[628]

Right to Be Forgotten

The legal principle, codified in Article 17 of the General Data Protection Regulation (GDPR), granting individuals the right to request erasure of personal data concerning them without undue delay. This privacy right enables data subjects to obtain deletion of personal information when specific conditions are met, including cases where data is no longer necessary for original processing purposes, consent is withdrawn, or processing has been unlawful, subject to balancing considerations including freedom of expression and legitimate public interest.[629]

Role

A named collection of permissions or abstract job function within an access control framework that can be assigned to users to streamline authorisation management. Roles represent organisational functions rather than individual identities, enabling systematic privilege allocation based on job responsibilities. For example, a "Manager" role might include permissions to view reports and approve requests, while an "Employee" role provides more limited access. This abstraction allows for dynamic permission management as users transition between organisational positions, supporting the principle of least privilege through precise entitlement grouping.[630]

Role-Based Access Control (RBAC)

A widely adopted access control paradigm that regulates system resource access through role assignments rather than direct user-permission mappings. Under RBAC, permissions are associated with organisational roles, and users acquire access rights by being assigned to appropriate roles. This model significantly reduces administrative

[628] National Institute of Standards and Technology, "Revocation" *Computer Security Resource Center Glossary*, accessed 1 April 2024, https://csrc.nist.gov/glossary/term/revocation.

[629] Ben Wolford, "Everything you need to know about the 'Right to be forgotten,'" *GDPR.eu*, 2025, https://gdpr.eu/right-to-be-forgotten.

[630] Ravi Sandhu, David F. Ferraiolo, and D. Richard Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard," in *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, Berlin, DE, July 26-27, 2000, 47-63, https://doi.org/10.1145/344287.344301.

complexity in large-scale environments while supporting security principles through hierarchical role structures and separation-of-duty constraints. RBAC implementations typically feature role hierarchies, where senior roles inherit permissions from subordinate roles, and constraints that prevent conflicting role assignments to individual users.[631]

Salting

Adding a unique, random value (at least 128 bits recommended) to each password before hashing so identical passwords produce different hashes, defeating pre-computed tables and cross-user comparisons. Use Argon2id or scrypt (memory-hard) for hashing; bcrypt and PBKDF2 remain widely deployed but are not memory-hard. Store salts alongside hashes.[632]

SAML 2.0

The Security Assertion Markup Language version 2.0 represents an XML-based standard for exchanging authentication and authorization data between security domains, particularly in federated identity scenarios. SAML 2.0 enables single sign-on through a trust triangle comprising Identity Providers (IdPs), Service Providers (SPs), and end users. The protocol supports both IdP-initiated and SP-initiated authentication flows, utilising cryptographically signed assertions to convey identity information. Key components include authentication statements, attribute statements, and authorisation decision statements, all protected through XML digital signatures and encryption mechanisms.[633]

Scoped Access Token

An access token within OAuth 2.0 and related authorisation frameworks that includes specific scope parameters limiting the token's permissions to predetermined resource access patterns. Scopes function as fine-grained authorisation constraints, enabling precise privilege boundaries for third-party applications. For instance, a token scoped to "read:calendar" permits calendar viewing but prohibits modification or access to other resources. This mechanism implements the principle of least privilege by ensuring

[631] Ravi Sandhu, David F. Ferraiolo, and D. Richard Kuhn, "The NIST Model for Role-Based Access Control: Towards a Unified Standard," in *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, Berlin, DE, July 26-27, 2000, 47-63, https://doi.org/10.1145/344287.344301.

[632] Paul A. Grassi et. al., 'Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management,' *National Institute of Standards and Technology*, June 2017, https://pages.nist.gov/800-63-3/sp800-63b.html.

[633] Organization for the Advancement of Structured Information Standards, *Security Assertion Markup Language [SAML] v2.0*, OASIS Standard, 15 March 2005, https://www.oasis-open.org/standard/saml/.

tokens grant only essential permissions, reducing potential damage from token compromise while enabling delegated authorisation scenarios.[634]

Seeding

The process of providing initial entropy or randomness to cryptographic systems, particularly deterministic random bit generators (DRBGs) and pseudorandom number generators. Seeding establishes the foundational unpredictability required for cryptographic key generation and secure random number production. High-quality seeds typically derive from hardware entropy sources or cryptographically secure random number generators, ensuring sufficient unpredictability for cryptographic applications. Proper seeding is critical for preventing predictable patterns in cryptographic operations and maintaining system security against statistical attacks.[635]

Self-Custodial Legal Identity

A digital identity management paradigm where individuals maintain direct control over their legal identity credentials without relying on continuous third-party verification services. This model enables users to store tamper-proof digital identity documents – such as government-issued IDs or educational certificates – in personal digital wallets. Users present these credentials directly to relying parties, who can cryptographically verify authenticity without contacting the original issuer. This approach enhances privacy and reduces dependency on centralised identity infrastructure while requiring users to assume responsibility for credential backup and recovery.[636]

Self-Sovereign Identity (SSI)

A comprehensive digital identity model granting individuals ultimate ownership and control over their identity data through decentralised infrastructure and cryptographic verification mechanisms. SSI eliminates dependence on centralised identity providers through a framework built on Decentralised Identifiers (DIDs), Verifiable Credentials, and blockchain-anchored trust. Users maintain digital wallets containing cryptographically verifiable credentials from multiple issuers, enabling selective disclosure and zero-knowledge proof presentations. The paradigm supports privacy-preserving identity

[634] D. Hardt, ed., "The OAuth 2.0 Authorization Framework," *Internet Engineering Task Force*, October 2012, https://datatracker.ietf.org/doc/html/rfc6749.

[635] Alexander H. Calis, Chris T. Celi, John Kelsey, Dr. Kerry McKay, Hamilton Silberg, and Dr. Meltem Sönmez Turan, NIST Special Publication 800-90A Rev. 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, National Institute of Standards and Technology, June 2015, https://csrc.nist.gov/projects/random-bit-generation.

[636] Evan Krul, Hye-young Paik, Sushmita Ruj and Salil S. Kanhere, "Trusting Self-Sovereign Identity," arXiv preprint, 10 April 2024, https://arxiv.org/html/2404.06729v1.

verification while enabling interoperable identity ecosystems across organisational boundaries.[637]

Secure Boot

A security mechanism ensuring that computing devices execute only cryptographically verified firmware and operating system components during the startup sequence. The secure boot process establishes a chain of trust from hardware-controlled code through successive boot stages, with each component verifying the digital signature of the next before execution. If signature verification fails, the boot process halts or enters recovery mode rather than executing potentially compromised code. This protection mechanism guards against rootkits, bootkits, and firmware-level malware by preventing execution of unauthorised code from the earliest system initialisation stages.[638]

Secure Element

A tamper-resistant hardware component designed to securely store sensitive data and execute cryptographic operations in isolation from the main system environment. Secure Elements typically feature dedicated microprocessors, secure memory, and physical countermeasures against tampering, side-channel attacks, and fault injection. Common implementations include chips in payment cards, SIM cards, and mobile devices for storing payment credentials, biometric templates, and cryptographic keys. The hardware design prevents unauthorised access to stored secrets even when the host system is compromised, providing a hardware root of trust for security-critical applications.[639]

Secure Enclave / Trusted Execution Environment (TEE)

Hardware-isolated execution environments within main processors that provide confidentiality and integrity guarantees for sensitive computations. TEEs create separate "secure worlds" with dedicated memory spaces and execution contexts isolated from the normal operating system environment. Examples include: ARM TrustZone and Intel Software Guard Extensions (SGX), which enable secure processing of cryptographic

[637] Roberto A. Pava-Díaz, Jesús Gil-Ruiz, Danilo A. López-Sarmiento, "Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation," *Frontiers in Blockchain* 7, 30 August 2024, https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2024.1443362/full.

[638] Vladimir Bashun, Anton Sergeev, and Victor Minchenkov, "Too young to be secure: Analysis of UEFI threats and vulnerabilities," in *Proceedings of the 14th Conference of FRUCT Association*, Espoo, Finland, November 11-15, 2013, https://www.researchgate.net/publication/269310822_Too_young_to_be_secure_Analysis_of_UEFI_threats_and_vulnerabilities.

[639] Carlton Shepherd, Ghada Arfaoui, Iakovos Gurulian, and Robert P. Lee, "Secure and Trusted Execution: Past, Present and Future—A Critical Review in the Context of the Internet of Things and Cyber-Physical Systems," *Future Internet* 8, no. 3, August 2016, https://www.researchgate.net/publication/306039236_Secure_and_Trusted_Execution_Past_Present_and_Future_--_A_Critical_Review_in_the_Context_of_the_Internet_of_Things_and_Cyber-Physical_Systems.

operations, biometric authentication, and digital rights management. Unlike standalone secure elements, TEEs leverage the main processor's computational power while maintaining security through hardware-enforced memory protection and cryptographic attestation mechanisms.[640]

Security Key

A hardware-based authentication device utilising cryptographic mechanisms to provide phishing-resistant multi-factor authentication. Security keys implement the FIDO2 standard, generating cryptographic key pairs where private keys remain secured within the device whilst public keys authenticate users across multiple applications without shared secrets between services.[641]

Serialisation

The computational process of converting data structures or object states into transmittable byte streams for storage or network transmission, enabling subsequent reconstruction in potentially different computing environments. This mechanism facilitates data persistence, distributed system communication, and cross-platform interoperability through standardised encoding formats.[642]

Session Fixation

A web application vulnerability exploitation technique wherein attackers predetermine session identifiers and manipulate victims into authenticating with these compromised tokens. The attack leverages inadequate session management protocols, allowing unauthorised access through hijacked validated sessions rather than credential theft.[643]

SIM-Swap

A telecommunications fraud methodology exploiting mobile carrier number portability features to redirect victim communications to attacker-controlled devices. This social engineering attack enables interception of SMS-based authentication codes, thereby

[640] Carlton Shepherd, Ghada Arfaoui, Iakovos Gurulian, and Robert P. Lee, "Secure and Trusted Execution: Past, Present and Future—A Critical Review in the Context of the Internet of Things and Cyber-Physical Systems," *Future Internet* 8, no. 3, August 2016, https://www.researchgate.net/publication/306039236_Secure_and_Trusted_Execution_Past_Present_and_Future_--_A_Critical_Review_in_the_Context_of_the_Internet_of_Things_and_Cyber-Physical_Systems.

[641] Hirsch, "Adopting Strong Passwordless Authentication by Using a FIDO Security Key," *Hirsch Security*, 6 March 2023, https://www.hirschsecure.com/resources/blog/adopting-strong-passwordless-authentication-by-using-a-fido-security-key

[642] Anuradha C and Arvind Padmanabhan, "Data Serialization," *Devopedia,* 24 July 2020, https://devopedia.org/data-serialization.

[643] mwood, Nsrav, Greenapple8189, KirstenS, Alan Jex, Mark Sienkiewicz, Bill Sempf and kingthorin, "Session fixation," *OWASP*, updated 5 January 2025, https://owasp.org/www-community/attacks/Session_fixation.

circumventing two-factor authentication mechanisms and facilitating account takeover scenarios.[644]

Siloed Identity

An architectural paradigm characterised by isolated identity management systems operating independently without integrated communication protocols. This fragmentation creates operational inefficiencies, duplicated data repositories, and compromised security visibility across organisational infrastructure components.[645]

Single Sign-On (SSO)

An authentication architecture enabling users to access multiple applications through centralised credential verification. SSO implementations utilise identity providers and service provider trust relationships, employing protocols such as SAML, OAuth, and OpenID Connect to facilitate seamless authentication whilst maintaining security boundaries.[646]

Smart Card

A portable cryptographic device containing embedded integrated circuits capable of storing, processing, and protecting digital credentials. These tamper-resistant hardware tokens implement public key infrastructure standards, providing strong multi-factor authentication through physical possession combined with PIN or biometric verification.[647]

Social Engineering

The systematic psychological manipulation of human behaviour to compromise security protocols and extract sensitive information. This attack methodology exploits cognitive biases, trust mechanisms, and social dynamics rather than technical

[644] Ibanibo Tamunotonye Sotonye, Nkechinyere Eyidia, and Wobiagери Ndidi Abidde, "Combating SIM Swap Fraud in Telecommunications: A Machine Learning Approach and Multi-Factor Authentication as a Preventive Strategy," *Journal of Advancement in Communication System* vol 8, no 2, May 2025, https://www.researchgate.net/publication/392902047_Combating_SIM_Swap_Fraud_in_Telecommunications_A_Machine_Learning_Approach_and_Multi-Factor_Authentication_as_a_Preventive_Strategy.

[645] Maryline Laurent-Maknavicius and Samia Bouzefrane, eds., *Digital Identity Management* (London: ISTE Press, 2015).

[646] Tayibia Bazaz and Aqeel Khalique, "A Review on Single Sign on Enabling Technologies and Protocols," *International Journal of Computer Applications* 151(11):18-25, October 2016, https://www.researchgate.net/publication/309225903_A_Review_on_Single_Sign_on_Enabling_Technologies_and_Protocols.

[647] Hamed Taherdoost and Maslin Masrom, "An Examination of Smart Card Technology Acceptance Using Adoption Model", *Proceedings of the ITI 2009 31st International Conference on Information Technology Interfaces*, Cavtat/Dubrovnik, Croatia, June 22-25, 2009, https://www.researchgate.net/publication/221238716_An_Examination_of_Smart_Card_Technology_Acceptance_Using_Adoption_Model.

vulnerabilities, representing a fundamental threat vector in contemporary cybersecurity landscapes.[648]

Social Graph Correlation

The analytical process of examining connections and relationships between individuals within social networks to identify, link, or infer information about specific entities. Social graph correlation employs relationship-mapping methodologies to connect distinct digital identities by analysing overlapping social connections, communication patterns, and network metadata across platforms. This technique can compromise anonymity even when explicit identifying information is absent, as correlation algorithms detect shared connection patterns that serve as quasi-fingerprints for identity linkage.[649]

Spoofing

The deliberate impersonation or falsification of identity markers, authentication credentials, or system characteristics to deceive recipients and bypass security mechanisms. Spoofing encompasses multiple attack vectors including email spoofing (falsifying sender addresses), IP spoofing (forging packet source addresses), GPS spoofing (broadcasting counterfeit positional signals), and biometric spoofing (presenting fabricated physiological identifiers). These attacks exploit trust relationships and authentication vulnerabilities to enable unauthorised access or misdirection of communications.[650]

Shadow Identity

A digital identity profile constructed from indirect data collection without the subject's explicit participation or awareness. Shadow Identities aggregate information from various sources, such as contact uploads, cross-platform data correlation, behavioural analytics, and third-party data brokers, and create comprehensive identity representations that exist independently of user-generated profiles. These constructs enable tracking and profiling capabilities that operate beyond traditional consent mechanisms, often employed for marketing attribution, risk assessment, or surveillance purposes.[651]

[648] Zuoguang Wang, Limin Sun, and Hongsong Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access* vol 8, 6 May 2020, https://ieeexplore.ieee.org/document/9087851.

[649] Pádraig MacCarron, Shane Mannion, and Thierry Platini, "Correlation distances in social networks," *Journal of Complex Networks* 3 vol 11, June 2023, https://academic.oup.com/comnet/article/11/3/cnad016/7197486.

[650] Sibi Chakkaravarthy Sethuraman, Devi Priya V S, Tarun Reddi, Mulka Sai Tharun Reddy, and Muhammad Khurram Khan, "A comprehensive examination of email spoofing: Issues and prospects for email security," *Computers & Security* vol 137, February 2024, https://doi.org/10.1016/j.cose.2023.103600.

[651] Luis Aguiar, Christian Peukert, Maximilian Schäfer, and Hannes Ullrich, "Facebook Shadow Profiles," arXiv preprint, 8 Feb 2022, https://arxiv.org/abs/2202.04131.

Subject

In identity management and access control contexts, the entity – typically an individual, service, or system process – that seeks to access protected resources within a computing environment. Subjects possess identity attributes and credentials that authentication systems verify before granting resource access. The term encompasses both human users and non-human entities (applications, services, devices) that require identity verification to interact with secured systems or data repositories.[652]

Surveillance Identity

A composite digital identity constructed through systematic monitoring and data aggregation across multiple platforms, sensors, and tracking mechanisms. Surveillance identities compile behavioural patterns, location data, communication metadata, transaction records, and biometric information to create comprehensive profiles used for monitoring, risk assessment, or predictive analysis. These constructs often incorporate information that subjects have not explicitly consented to share and may be utilised for targeting, enforcement, or commercial purposes without the subject's knowledge or control.[653]

Suspension

The temporary deactivation of user accounts or identity credentials that prevents authentication and resource access whilst preserving the underlying identity record. Suspension serves as an intermediate security measure between active access and permanent account deletion, typically implemented in response to security incidents, policy violations, or during investigations. Suspended identities maintain their associated attributes and access rights in an inactive state, enabling restoration without requiring complete re-provisioning of permissions and credentials.[654]

Sybil Attack

A coordinated attack wherein a single malicious entity creates multiple fraudulent identities to subvert decentralised systems that rely on consensus mechanisms or reputation-based trust. The attack exploits the fundamental assumption that distinct network identities correspond to separate entities, enabling the attacker to

[652] Paul A. Grassi et al., *Digital Identity Guidelines* [NIST Special Publication 800-63-3, June 2017], https://pages.nist.gov/800-63-3/.

[653] Victoria Wang and John V. Tucker, *Formalising Surveillance and Identity*, arXiv preprint, 14 August 2014, https://arxiv.org/abs/1408.4858.

[654] Paul A. Grassi et al., D*igital Identity Guidelines: Enrollment and Identity Proofing* [SP 800-63A], National Institute of Standards and Technology, June 2017, https://pages.nist.gov/800-63-4/sp800-63a.html.

disproportionately influence voting systems, compromise peer-to-peer networks, or manipulate reputation mechanisms through identity multiplication.[655]

Synthetic Identity

A fabricated persona constructed through the strategic combination of legitimate personally identifiable information with falsified credentials, creating a fictitious identity that passes automated verification systems whilst remaining untraceable to any actual individual. Distinguished from traditional identity theft, synthetic identities represent entirely manufactured entities designed to exploit gaps in identity verification protocols.[656]

Systems Modelling

The methodological creation of abstract representations of complex systems to analyse component interactions, system behaviour, and emergent properties through formal or semi-formal frameworks. In identity systems contexts, encompasses the documentation of authentication flows, trust relationships, and data propagation patterns to facilitate design validation, threat analysis, and stakeholder communication.[657]

Token (Cryptography)

A cryptographic artifact representing authenticated credentials or authorisation permissions, providing time-limited access to protected resources following successful authentication. Distinguished from passwords by its temporal nature and possession-based verification model, tokens eliminate the requirement for repeated credential validation whilst maintaining granular access control.[658]

Token (Web3)

A cryptographic unit recorded on a blockchain (and governed by smart contracts) that represents transferable claims, such as value, access rights, or participation in a protocol. Tokens are typically fungible (interchangeable units, e.g., ERC-20) or non-fungible (unique items, e.g., ERC-721), with hybrid forms (e.g., ERC-1155). In digital identity contexts, they may be used for token-gated access or to carry attestations, but

[655] John R. Douceur, "The Sybil Attack," in *Proceedings of the First International Workshop on Peer-to-Peer Systems*, January 2002, Microsoft Research, https://www.microsoft.com/en-us/research/publication/the-sybil-attack/.

[656] Federal Reserve Banks, "What Is Synthetic Identity Fraud?" *FedPayments Improvement*, 2025, https://fedpaymentsimprovement.org/resources/focus-areas/synthetic-identity-fraud.

[657] International Council on Systems Engineering [INCOSE], "MBSE Initiative: Model-Based Systems Engineering [MBSE]," INCOSE, 2025, https://www.incose.org/initiatives/mbse-initiative.

[658] Dick Hardt, ed., *The OAuth 2.0 Authorization Framework* [RFC 6749], Internet Engineering Task Force, October 2012, https://www.rfc-editor.org/rfc/rfc6749.html.

transferability, key loss/recovery, and market incentives make them brittle and vulnerable to social-engineering abuse.[659]

Threat Model

A structured analytical framework identifying potential adversaries, attack vectors, and system vulnerabilities within a specific operational context. The methodology systematically enumerates threat agents, their capabilities and motivations, probable attack pathways, and organisational assets at risk, enabling prioritised security control implementation and risk mitigation strategies.[660]

Trust

The reliance upon the integrity and reliability of an entity or system without independent verification requirements. In digital identity contexts, represents the acceptance of assertions regarding identity, credentials, or system behaviour based on established confidence in the asserting party's verification processes and security posture.[661]

Trust Anchor

An authoritative cryptographic entity serving as the foundational point of trust within hierarchical security systems, particularly public key infrastructures. Represents a self-signed certificate or root authority whose trustworthiness is assumed rather than derived, establishing the basis for all subsequent certificate chain validation and cryptographic trust relationships.[662]

Trust Framework

A comprehensive governance structure establishing standardised rules, technical specifications, and operational requirements enabling secure interoperability among multiple identity providers and relying parties. Encompasses legal agreements, assurance levels, certification processes, and technical protocols that facilitate mutual recognition of digital credentials across organisational boundaries.[663]

[659] Fabian Vogelsteller and Vitalik Buterin, "ERC-20: Token Standard," *Ethereum Improvement Proposals*, EIP-20, accessed 21 August 2025, https://eips.ethereum.org/EIPS/eip-20.

[660] Microsoft Corporation, "Threat Modeling," *Microsoft Security Development Lifecycle*, 2025, https://learn.microsoft.com/en-us/security/devsecops/threat-modeling.

[661] Paul A. Grassi et al., *Digital Identity Guidelines* [SP 800-63-4], National Institute of Standards and Technology, draft 2024, https://pages.nist.gov/800-63-4.

[662] Paul A. Grassi et al., *Digital Identity Guidelines* [SP 800-63-4], National Institute of Standards and Technology, draft 2024, https://pages.nist.gov/800-63-4.

[663] "Digital Identity and Attributes Trust Framework," GOV.UK, 13 September 2024, updated 26 June 2025, https://www.gov.uk/government/publications/digital-identity-and-attributes-trust-framework.

Two-Factor Authentication / One-Time Password

A security enhancement requiring users to present credentials from two distinct authentication factor categories for access verification. Two-Factor Authentication (2FA) requires *two distinct factors* (know/have/are). One-Time Passwords (OTP) are *short-lived codes* (time-based or event-based) often used as the possession factor in 2FA, but OTP ≠ 2FA by itself. Phishing-resistant 2FA is best achieved with FIDO2/WebAuthn security keys or passkeys.[664]

Unlinkability

A privacy property wherein an attacker cannot sufficiently distinguish whether items of interest within a system are related. The capability to prevent correlation between disparate identity attributes, transactions, or digital interactions, ensuring that separate actions or identities remain dissociated from an observer's perspective. This property proves fundamental to privacy-preserving identity architectures, enabling users to maintain contextual separation between different aspects of their digital presence whilst preventing unauthorised profiling through cross-domain correlation.[665]

User

An individual or entity that interacts with digital systems, services, or applications through authenticated or anonymous sessions. Within identity management contexts, the user represents the human subject whose identity attributes, credentials, and access permissions constitute the foundation of authentication and authorisation decisions. Users encompass diverse stakeholder categories including employees, customers, partners, and citizens, each requiring appropriate identity assurance levels commensurate with their access requirements and associated risk profiles.[666]

User Agent

Any client programme that initiates requests within networked communication protocols, particularly HTTP. The term encompasses web browsers, mobile applications, automated scripts, IoT devices, and any software acting on behalf of users in client-server architectures. User agents identify themselves through standardised headers containing

[664] Paul A. Grassi et al., *Digital Identity Guidelines: Authentication and Lifecycle Management* (SP 800-63B), National Institute of Standards and Technology, June 2017 (updated 2020), https://pages.nist.gov/800-63-3/sp800-63b.html; Communications Security Establishment, *Guideline on Multi-Factor Authentication* (ITSP.30.031), Government of Canada, April 2023, https://cyber.gc.ca/en/guidance/itsp30031-guidance-use-multi-factor-authentication.

[665] Andreas Pfitzmann and Marit Hansen, "A Terminology for Talking about Privacy by Data Minimization," Internet Engineering Task Force, 23 August 2010, https://www.ietf.org/archive/id/draft-hansen-privacy-terminology-00.txt.

[666] National Institute of Standards and Technology (NIST) Computer Security Resource Center, "User," *Glossary*, 2024, https://csrc.nist.gov/glossary/term/user.

product tokens and version information, enabling servers to tailor responses for compatibility whilst creating potential privacy implications through device fingerprinting. Modern user agents extend beyond human-operated browsers to include autonomous systems conducting background operations without direct user interaction.[667]

Vein Pattern

A biometric using subcutaneous vascular patterns (e.g., palm/finger) imaged with near-infrared light. Internal anatomy provides inherent liveness and robustness to spoofing; reported false-accept rates are low in vendor evaluations, but performance varies by implementation and conditions.[668]

Vendor

A commercial entity providing identity management technologies, platforms, or services within the digital identity ecosystem. Vendors encompass solution providers offering authentication systems, identity verification services, biometric technologies, and identity governance platforms to organisational clients. These entities shape identity infrastructure through proprietary implementations whilst navigating tensions between interoperability requirements and competitive differentiation. Vendor lock-in represents a persistent concern as organisations become dependent on specific technical architectures and data formats, potentially constraining future migration options and creating systemic dependencies within identity ecosystems.[669]

Verifiable Credential (VC)

A tamper-evident credential whose authorship can be cryptographically verified, enabling secure digital representation of traditionally physical credentials. Verifiable credentials implement W3C standards for expressing claims about subjects through digitally signed attestations from authoritative issuers, supporting selective disclosure and privacy-preserving presentation. The architecture comprises three roles: issuers who create credentials, holders who control them, and verifiers who validate them, establishing a trust triangle independent of centralised intermediaries. This paradigm enables portable, user-controlled identity attributes whilst maintaining cryptographic assurance of authenticity and integrity.[670]

[667] Roy T. Fielding, Mark Nottingham, and Julian Reschke, 'RFC 9110: HTTP Semantics,' *Internet Engineering Task Force*, June 2022, https://www.rfc-editor.org/rfc/rfc9110.html.

[668] ISO/IEC JTC1 SC37, 'Biometrics Standards Development,' *International Organization for Standardization, ongoing*, https://www.iso.org/committee/313770.html.

[669] *Oxford Advanced Learner's Dictionary,* s.v. "vendor," updated 21 August 2025, accessed 22 August 2025, https://www.oxfordlearnersdictionaries.com/definition/english/vendor.

[670] Manu Sporny, et al., 'Verifiable Credentials Data Model v2.0,' *World Wide Web Consortium*, 15 May 2025,

Verifier

A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for processing and validation. The verifier evaluates cryptographic proofs, checks credential status, and determines whether presented claims satisfy requirements for granting access or services. Also termed a relying party in federated identity contexts, verifiers must establish trust relationships with credential issuers whilst implementing appropriate validation mechanisms to prevent presentation attacks and ensure credential freshness.[671]

Verification

The evaluation of whether a verifiable credential or verifiable presentation constitutes an authentic and current statement of the issuer or presenter respectively. This process encompasses conformance checking against specifications, validation of cryptographic securing mechanisms, and status verification through revocation registries. Verification establishes technical validity without implying evaluation of claim truthfulness, distinguishing cryptographic authenticity from semantic accuracy. The verification process forms a critical component of trust establishment whilst remaining distinct from identity proofing or authorisation decisions.[672]

Voiceprint

A mathematical model extracted from human speech patterns serving as a biometric identifier through analysis of vocal characteristics including pitch, cadence, and frequency distributions. Voice biometric systems create enrollment templates from multiple speech samples, subsequently comparing new utterances against stored voiceprints to establish identity matches above confidence thresholds. Modern implementations leverage neural networks for text-independent recognition achieving accuracy rates exceeding 99% whilst remaining vulnerable to presentation attacks through recordings or synthetic voice generation. ISO/IEC 30107 standards address anti-spoofing requirements through liveness detection mechanisms.[673]

https://www.w3.org/TR/vc-data-model-2.0/.

[671] Manu Sporny, et al., 'Verifiable Credentials Data Model v2.0,' *World Wide Web Consortium*, 15 May 2025, https://www.w3.org/TR/vc-data-model-2.0/.

[672] Manu Sporny, et al., 'Verifiable Credentials Data Model v2.0,' *World Wide Web Consortium*, 15 May 2025, https://www.w3.org/TR/vc-data-model-2.0/.

[673] Andreas Nautsch, et al., 'Preserving privacy in speaker and speech characterisation,' *Computer Speech & Language*, 2019, November 2019, https://www.sciencedirect.com/science/article/pii/S0885230818303875.

Watchlist / Denylist / Blacklist

Lists of entities, identifiers, or attributes designated for special handling, restriction, or prohibition within identity and access management systems. Denylists (formerly blacklists) enumerate explicitly forbidden items requiring blocking, whilst allowlists specify exclusively permitted entities. Watchlists trigger enhanced monitoring or additional verification requirements without necessarily preventing access. Contemporary practice favours inclusive terminology with 'denylist' replacing 'blacklist' to eliminate exclusionary language whilst maintaining functional clarity. Implementation strategies balance security effectiveness against maintenance overhead and false positive rates.[674]

Web 2.0

A paradigm shift in web architecture characterised by user-generated content, collaborative platforms, and dynamic interaction replacing static publishing models. Coined by Tim O'Reilly in 2004, Web 2.0 transformed the internet from read-only consumption to read-write participation through social media, wikis, and cloud services. This evolution leveraged network effects and collective intelligence whilst concentrating power within platform intermediaries who monetised user data and attention. The Web 2.0 model established surveillance capitalism's foundations through behavioural tracking and targeted advertising, creating walled gardens that contradicted early internet decentralisation ideals.[675]

Web3

A proposed internet architecture leveraging blockchain technology, cryptographic protocols, and token economies to enable decentralised ownership and governance. Conceived by Ethereum co-founder Gavin Wood in 2014, Web3 envisions trustless peer-to-peer interactions eliminating platform intermediaries through smart contracts and distributed consensus mechanisms. The paradigm promises user sovereignty over data and digital assets whilst critics highlight scalability limitations, environmental impacts, and wealth concentration among early adopters. Web3's realisation remains contested between genuine decentralisation advocates and venture-backed projects reproducing Web 2.0's extractive dynamics with cryptocurrency speculation.[676]

[674] Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, 'NIST Special Publication 800-167. Guide to Application Whitelisting,' *National Institute of Standards and Technology*, October 2015, https://csrc.nist.gov/pubs/sp/800/167/final.

[675] Tim O'Reilly, 'What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software,' *O'Reilly* Media, 30 September 2005, https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

[676] Dr. Gavin Wood, 'Ethereum: A Secure Decentralised Generalised Transaction Ledger,' *Ethereum Foundation*, 2014, https://ethereum.github.io/yellowpaper/paper.pdf.

WebAuthn

A W3C API that lets web apps use strong, attested public-key credentials (passkeys, roaming security keys) for passwordless or second-factor authentication. Credentials are bound to the site's origin, providing phishing resistance and eliminating shared secrets. [677]

Zero-Knowledge

A cryptographic method enabling one party to prove knowledge of information without revealing the information itself. Introduced by Goldwasser, Micali, and Rackoff in 1985, zero-knowledge proofs convey only the validity of a statement whilst preserving complete confidentiality of underlying data. These protocols satisfy three properties: completeness (honest provers convince honest verifiers), soundness (dishonest provers cannot convince honest verifiers), and zero-knowledge (verifiers learn nothing beyond statement validity). Applications span from privacy-preserving authentication to selective disclosure in digital credentials, enabling cryptographic proof of attributes without exposing sensitive personal information.[678]

[677] Jeff Hodges, et al. 'Web Authentication: An API for accessing Public Key Credentials Level 3,' *World Wide Web Consortium*, 2024, https://www.w3.org/TR/webauthn-3/.

[678] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, 'The knowledge complexity of interactive proof systems,' *SIAM Journal on Computing* 18, no. 1 (1989): 186-208, https://epubs.siam.org/doi/10.1137/0218012.

Appendix B. Research interview questions

NDC DIGITAL IDENTITY PARTICIPATORY INTERVIEW

Each interview is conducted via a platform selected by the participant, and facilitated by two researchers. Interviews are recorded by both facilitators using OBS Studio to record and save locally. Participants are asked to consent to the interview in advance via the Research Consent Form.

Interviews are unstructured, and should follow the top level numbering where possible. Given the time frame for each interview, it is likely that not all questions documented here will be covered.

Pre-Interview Checklist

	CONSENT FORM ON FILE - ADD LINK HERE
	PARTICIPANT EXPECTATIONS SET
	PARTICIPANT CONFIRMS PARTICIPATION RIGHTS
	COMPLETED ENVIRONMENT CHECK
	COMPLETED EQUIPMENT CHECK
	SILENCE DEVICES AND NOTIFICATIONS

Interview guide

1. Introductions & technical check

a. Facilitator introductions (use biographies from team site and ensure that external researchers have a pre-approved biography).

b. Confirm how long the participant has scheduled for their interview.

c. Explain the purpose of the interview:

i. Recap the research goals.

ii. Cover the **core framing** of the case study research:
Biometrics, Decentralisation, Financialisation, Political, Physical, Decision making and Implementation.

iii. Remind the participant of the code of conduct and the research methodology and commitment to confidentiality.

iv. Review the Research Consent Form between participant and facilitators.

v. Confirm with participant that the interview can be terminated at any point, and/or that the interview can be conducted off-record.

d. Ask if the participant has any questions.

e. Ask for secondary recorded verbal consent from participant.

2. Setting the stage – Participant introduction

Inform the participant that the recording has started.

a. What is your role?
How long have you been involved in the disciple of Digital Identity?

b. What motivates your work in Digital Identity?

c. Have you ever worked on:

i. a digital identity project before this one?

ii. a infrastructure project with ambitions of scale?

3. Participant perspective of digital identity

a. What is your definition of digital identity?

b. Why do you think digital identity is important? What is its role?

c. Can you detail a digital identity system that you think is particularly...

i. efficient, powerful, secure or reliable

ii. dangerous, vulnerable, hostile to users

4. Participant reflection of key terms

a. Describe your understanding of these terms, and take a moment to describe a positive and negative example of each term:

i. Biometrics

ii. Pseudonymity / Anonymity

iii. Authentication

iv. Recognition

v. Federation

vi. Decentralisation

vii. Digitisation/serialisation

viii. Financialisation/assetisation

b. For each of these terms, when does the positive outweigh the negative, and vice versa?

5. Setting the stage for threat modelling

a. Why are current digital identity implementations broken?

b. Detail an example — either real or theoretical — that concerns you about a digital identity system.

i. What kind of harm would this concern cause?

ii. Who would be harmed?

iii. In your view, can the risk be mitigated?

6. Participant work reflection

a. Please describe a recent project that you worked on.

i. What were its goals?

ii. What tools were used?

iii. What were its successes?

iv. What were its failures?

v. How were the successes and failures documented and discussed?

vi. Was there anything that did not get discussed?

7. Uncovering anxieties

Offer a content warning, reiterate participant control and refer to the participants statement rights.

a. Have you ever encountered something in [the code/the hardware/strategy] that has given you cause for concern?

b. Have you ever felt unsafe or experienced a threat while working with this project?

c. Have you ever felt concerned for the resilience, safety or integrity of policymakers/users/decisionmakers/technologists?

d. Have you ever woken up in the middle of the night thinking about your work?

8. Threat modelling with the participant

a. Thinking about your most recent work/shared anxiety:

i. How could your project be weaponized to target you?

ii. How could your project be weaponized to target your organization?

iii. What would be the easiest way to destroy your work? What would the implications be if this happened?

iv. What would the implications be if your work continued in operation for 10/50/100 years?

9. Institutional consent

a. In your opinion, are the goals expressed by the broader digital identity landscape possible within the current trajectory of the project?

b. Are you aware of any dedicated set of policies and guides as part of their value statements?

c. Do you check or otherwise critically examine your work or the work of others? What works, and what doesn't?

10. Looking outwards and forward

a. Thinking about what we have covered today, are there any institutions whose practices you admire and would like to adopt?

b. Who is the biggest threat in digital identity?

c. Are there any broader social issues now or on the horizon (eg pandemic, climate, warfare, injustice etc) that you feel are not being considered?

11. Final thoughts

a. Anything we haven't covered today?

12. Wrap up

a. Inform the participant that the recording has stopped.

b. Debrief, describe next steps.

c. Check in case the participant wishes to speak off the record.

Appendix C. Sample participant outreach

Step 1 – Initital Outreach

Hi [name],

My name is [name], and I am [role] at New Design Congress. We are an independent research group confronting the gap between what is said to be happening and what is *actually happening* within digitised societies.

We discovered your work from [insert article/essay/book/reason] and found it incredibly compelling. Following on from our research into data custodianship and digital consent, we are now engaged in a year-long research project aimed at exploring the socio-political implications of current and emergent forms of digital identity.

Our primary objective is to provide a comprehensive analysis of digital identity, viewing it as a contemporary form of governmental and capitalist rationality: identity systems as operations of statecraft, biometrics and information security, so-called 'Proof of Personhood'/'Proof of Life', individual serialisation, crisis-led adoption, cultural mismatches, as well as consent.

We are looking to conduct on-the-record and/or off-the-record interviews of actors involved in this broad field. Your work especially [cite work touching on a topic related to DID] touches on a facet of the issue we'd love to be able to discuss further. We would greatly value the opportunity to meet with you in the next few weeks. Our aim is to foster broader discussions and open our findings to increased civil society scrutiny.

Finally, in the interest of full disclosure, this research project is supported at various levels by the Signal Foundation (2023), Aspiration (2022-2023), Tools for Humanity (2023), Protocol Labs/Filecoin Foundation (2022), The Radicle Foundation (2021) and Public Office (2020), alongside dozens of individual members of the NDC community.

We look forward to hearing from you.

Warm regards,

PS: You can read more about New Design Congress and our team here, along with the policies that govern our work: our Research Methodology, Privacy Policy and Code of Conduct.

Step 2 – Invitation

Dear [Name],

My name is [name], and I am [role] at New Design Congress.

Thank you for providing your contact details to participate in our digital identity research project. We would greatly value the opportunity to meet with you in the next few weeks for a research interview.

If you are still interested and have availability for a 1+ hour interview, please book an available timeslot by visiting https://[redacted-link]/digital-identity-research-interview and finding a time that will best suit you.

Please take a moment to read the Participant Bill of Rights and Consent Form located here: https://[redacted-link]/participant-bill-of-rights. **You will need to sign and return a copy of the consent form prior to the interview.**

Finally, you can find more about how we conduct our research via these three links:

- Research methodology: https://newdesigncongress.org/en/methodology/
- Code of conduct: https://newdesigncongress.org/en/conduct/
- Privacy policy: https://newdesigncongress.org/en/privacy/

Please do not hesitate to contact us with any questions or clarifications.

We look forward to speaking with you!

Kind regards,

Appendix D. Research Consent Form

RESEARCH PARTICIPATION CONSENT FORM

You are invited to take part in a research study with personnel from New Design Congress. Please read this form carefully, or have someone read it to you, and ask any questions you may have before agreeing to take part in this interview. If the consent form is read to the interviewee, either in English or another language, please also have a witness who was present for the reading sign below.

If you have any concerns or questions about the consent form, please contact us at consent@newdesigncongress.org.

The purpose of this interview/research is to discuss possible collaboration and civil society engagement around the topic of digital identity systems, based on the ongoing research by New Design Congress. We are interviewing members of project teams and other ecosystem stakeholders to get a broad range of insights and opinions around how projects consider and undertake usability and design initiatives in their work.

With your permission, we would like to take handwritten notes, record using OBS or the platform of your choice, and transcribe the audio using local transcription. The recordings and transcripts will be used solely for review and analysis purposes. We will not share raw notes or recordings made with anyone outside of New Design Congress, and any excerpted information or quotations that are used in presentations or publications will be made anonymous. Still, if you wish, you may choose to participate without being recorded, in which case we will only take notes. We will keep the recordings in password-protected storage until the project has been completed, and for an additional two months. We will destroy all recorded material by **1 September 2024**.

You can read more about our approach to privacy at https://newdesigncongress.org/en/privacy

Reimbursement: We are offering compensation for your time (up to 2 hours) and insight in the form of a 350€ payment into your bank account. Please include your bank account details when returning this form. Compensation will be paid 30 days after the completion of your participation.

Risk to you as a participant: There will be no invasion of privacy as a result of this research. Any transcriptions that are made of an audio or video recording will have all identifying information removed. Access to the original photos will be restricted to New Design

Congress, unless you give us written permission otherwise. We will take all necessary and appropriate precautions to limit any risk of your participation.

Taking part is voluntary: Taking part in an interview with New Design Congress is completely voluntary. You do not have to answer any questions you do not feel comfortable answering. You may instruct the interviewer to stop the interview at any time, in which case no subsequent actions performed by you will be included in our project or publications. You may also instruct New Design Congress to destroy all record of your participation at any time.

Confidentiality: Anything that we make public about our research will not include any information that will make it possible to identify you. Your name, address, and other personal information will not appear in any transcriptions of this interview, and they will not be released to anyone without your written permission. Research records will be kept in a secure location, and only New Design Congress personnel will have access to them.

Methodology and code of conduct: We adhere to a transparent, open and rigorous research methodology, backed up by our code of conduct that governs all New Design Congress activities, including research. You can read both of these documents online at https://newdesigncongress.org/en/methodology and https://newdesigncongress.org/en/conduct

Please read and sign the Statement of Consent on the next page.

Participant Bill of Rights

1. I can ask questions about the interview, the organization, or the interviewer atany time.
2. I do not have to answer any question that I do not want to.
3. I can refuse to be video or audio recorded and I will still be compensated.
4. I can leave at any time and I will still be compensated.
5. I can provide confidential feedback on my interview experience to New Design Congress.
6. I must approve the use of any photos, audio, videos or anonymised quotes that are used publicly, whether on a website, on a blog, or in the press.
7. Once a photo, video or quote has been published, I have the right to request it be taken down at any point in the future.

Statement of Consent

- I have read this form or it has been read to me.
- I have had the opportunity to ask questions and any questions that I have asked have been answered to my satisfaction.
- I understand my rights as a participant.
- I consent voluntarily to participate in this interview and any information I provide or audio or video recordings that are made may be used in the manner described above.

SIGNATURE:

NAME: ______________________ DATE:______________

ETHICAL DESIGN?
NO THANKS
NEWDESIGNCONGRESS.ORG