Digital Identity and Inclusion

Digital Identity and Inclusion: Tracing Technological Transitions

Emrys Schoemaker, Aaron Martin, and Keren Weitzberg

[This is an open-access version. The published version is available here: https://muse.jhu.edu/article/897699/summary]

Abstract

It is increasingly challenging for policymakers and other stakeholders to appreciate the growing complexity of the digital identity ecosystem, the technologies involved, and the broad implications of their deployment. This article seeks to help clarify these current debates and controversies by highlighting some of the technological transformations that are underway in the sector. We trace the ongoing transitions from "Big ID" systems to self-sovereign identity (SSI) approaches and digital wallets to the recent emergence of super apps, analyzing the different geographies of these systems and their impacts on exclusion and power relations. We argue that all technologies are political, and digital identity technologies especially so. Despite recent moves towards decentralization couched in the rhetoric of individual empowerment, most systems continue to exhibit features of centralization and tend to reinforce existing institutional arrangements.

Introduction

In June 2022, New York University's Center for Human Rights and Global Justice published a highly critical report, *Paving a Digital Road to Hell?*, which rebuked the World Bank and, in particular, its Identification for Development (ID4D) program for promoting digital identity systems in "Global South" countries without ensuring sufficient protections for human rights.[1] The report's publication reinvigorated a debate among international organizations, civil society groups, and other stakeholders about the role of digital identity in our societies and economies. Digital identity systems–i.e., systems in which identification, authentication, or authorization are performed digitally[2]–are becoming increasingly central to how people around the world access government services, welfare, aid, finance, and even connectivity, particularly across the Global

[1] Center for Human Rights and Global Justice, NYU Law School, *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID* (June 2022), https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf.

[2] Carly Nyst, Steve Pannifer, Edgar Whitley, and Paul Makin, *Digital Identity: Issue Analysis*. PRJ.1578 (Consult Hyperion, 8 June 2016), 28-29, https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

South. In their categorization of individuals, they are also reshaping the very way personal identity is understood, managed, and institutionally verified. Digital identity systems mediate the citizen-state relationship, making civil-rights considerations and socioeconomic inclusion key issues for decision-makers and the public.

In addition to centering concerns about the lack of human-rights protections in emerging digital identity infrastructures, the NYU report also put a critical focus on the influential role of powerful actors like the World Bank in advancing new projects. While the World Bank is undoubtedly an important player in this space, it is not alone in advocating internationally for digital identity initiatives. A closer look at this ecosystem reveals an ever-expanding group of actors, alliances, and partnerships, such as the ID2020 Alliance, the Secure Identity Alliance, and ID4Africa[3] (a self-described "NGO movement"), among many others, whose purpose is to promote the development and implementation of digital identity technologies in different contexts.

As experts in this space, we observe that it is increasingly challenging for policymakers and other stakeholders to appreciate the growing complexity of the digital identity ecosystem, the technologies involved, and the broad implications of their deployment. This article, therefore, gives context to current debates and controversies by highlighting some of the technological transformations underway in the sector–tracing the ongoing transitions from "Big ID" systems to self-sovereign identity (SSI) approaches and digital wallets to the recent emergence of super apps. We examine the ideologies that underpin and motivate the adoption of digital identity technologies, highlight their surveillance implications,[4] and briefly assess their impacts on socio-economic inclusion and exclusion. In what follows, we raise three key questions:

1) How are digital identity technological transformations impacting socioeconomic development?
2) What ideologies govern these transformations (implicitly or explicitly)?
3) What surveillant, inclusionary, and exclusionary effects are emerging?

We conclude by reflecting on the different geographies of these systems and their impacts on exclusion and power relations. In short, we argue that all technologies are political, and digital identity technologies especially so. Despite recent moves towards decentralization couched in the rhetoric of individual empowerment, most systems continue to depend on state-issued legal identities for value to both users and relying

[3] https://id2020.org; https://secureidentityalliance.org; https://id4africa.com.
[4] cf. Keren Weitzberg, Margie Cheesman, Aaron Martin, and Emrys Schoemaker, "Between Surveillance and Recognition: Rethinking Digital Identity in Aid," *Big Data and Society* 8, no. 1 (2021). doi: 10.1177/20539517211006744.

parties. All three models discussed below exhibit some features of centralization. We argue that technologies tend to reinforce existing institutional arrangements. However, the more immature and untested the innovation and abstracted from avenues of public critique and redress, the more exclusion and power imbalances are amplified. While digital identity systems can – and should – be designed to benefit people by strengthening their access to services and entitlements, too often a lack of understanding of user needs and local context shapes uptake and use, to the detriment of meaningful inclusion. We thus urge attention to questions of institutional interests, device access, and user capability in the pursuit of inclusive digital identity systems.

The dawn of Big ID

"Big ID," a term first coined by the civil society group Access Now,[5] refers to centralized biometric systems. Often implemented in regions where people historically lack robust forms of legal identification, they have gained widespread institutional support over the last two decades. Typically funded by international actors, these programs are implemented by both national governments and international humanitarian and aid organizations. Examples include humanitarian initiatives such as the UN World Food Programme's biometric aid delivery system (known as SCOPE); national ID programs like India's Aadhaar and Kenya's Huduma Namba project; and biometrically administered welfare programs such as Bolsa Familia in Brazil. The "biometric turn" has been celebrated as a route towards achieving UN Sustainable Development Goal 16.9 ("legal identity for all") and empowering the poor.[6]

Critics of the centralized collection of sensitive biometric data have pointed to various risks of abuse and misuse centered around data governance, privacy, security, and surveillance issues. Civil society groups and digital rights advocates have argued that Big ID systems are particularly vulnerable to data breaches, facilitate inappropriate data-sharing with third parties, and enable unprecedented forms of data linking and tracking, which can be used to target migrants, political dissidents, and other vulnerable individuals and groups.[7]

The large-scale centralized models underpinning Big ID systems–often aimed at reducing "leakage" and streamlining distribution across large populations–also tend to pose particular problems of exclusion. Take Aadhaar, for example. Aadhaar is the

---

[5] Access Now, "Big ID, bad idea: busting ID myths that are endangering human rights." Press Release, 5 October 2021, https://www.accessnow.org/big-id-endangering-human-rights.

[6] Alan Gelb and Julia Clark, "Identification for development: The biometrics revolution," *Center for Global Development Working Paper* 315 (2013).

[7] "Biometrics: Who's Watching You?" Electronic Frontier Foundation (EFF), 14 September 2003, https://www.eff.org/wp/biometrics-whos-watching-you; and The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector* (March 2018), https://theengineroom.org.

world's most extensive biometric identification program. Hindi for "foundation," it is a 12-digit identification number issued by the Unique Identification Authority of India. In and of itself, it does not confer any benefits. Instead, its main goal is to verify the "selfsameness" of the person.[8] Nowadays, to be registered for an Aadhaar number, one must provide a range of biographical details in addition to several types of biometrics–a facial photo, ten fingerprints, and two iris scans.

First launched in 2009, Aadhaar has become a prerequisite for accessing a range of public and private services in India.[9] Though technically non-compulsory, having an Aadhaar number is often sarcastically deemed "voluntarily mandatory."[10] Intended as an anti-fraud device for eliminating duplicate and "ghost" beneficiaries, the Aadhaar system has largely put the onus on individuals to register and resolve technical errors rather than placing responsibility on the state to ensure no one is denied access to essential services. This focus on inclusion (rather than exclusion) errors has often obstructed welfare access.[11] From the very start, Aadhaar was met with complaints about technical failures leading to rightful beneficiaries being denied government services, such as food rations.[12] In extreme cases, Aadhaar denial has been linked to starvation.[13]

These problems are linked, at least in part, to system and technical design. Many biometric technologies are implicitly designed with able-bodied subjects in mind.[14] Manual workers and the elderly, whose aged eyes and calloused fingerprints make biometric capture and authentication a challenge, are at particular risk.[15] A 2016 household survey in the Indian state of Jharkhand found that "elderly couples and

---

[8] Ursula Rao and Vijayanka Nair, "Aadhaar: Governing with biometrics," *South Asia: Journal of South Asian Studies* 42, no. 3 (2019): 475.
[9] Silvia Masiero, "Digital governance and the reconstruction of the Indian anti-poverty system," *Oxford Development Studies* 45, no. 4 (2017): 393-408.
[10] "Voluntarily Mandatory," *The Hindu*, 30 September 2013, https://www.thehindu.com/opinion/editorial/voluntarily-mandatory/article5182756.ece.
[11] Jean Drèze and Reetika Khera, "Recent social security initiatives in India," *World Development* 98 (2017): 555-572; and Silvia Masiero and Soumyo Das, "Datafying anti-poverty programmes: Implications for data justice," *Information, Communication & Society* 22, no. 7 (2019): 916-933.
[12] Anumeha Yadav, "On the Margins of Aadhaar: The Living Dead, and Food 'Disruptions'," in *Dissent on Aadhaar: Big Data Meets Big Brother*, ed. Reetika Khera (New Delhi: Orient Blackswan); and Silvia Masiero, "Biometric infrastructures and the Indian public distribution system," *South Asia Multidisciplinary Academic Journal* 23 (2020), https://journals.openedition.org/samaj/6459.
[13] Shiv Sahay Singh, "Death by digital exclusion?: On faulty public distribution system in Jharkhand," *The Hindu*, 13 July 2019, https://www.thehindu.com/news/national/other-states/death-by-digital-exclusion/article28414768.ece.
[14] Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Duke University Press, 2011).
[15] Jean Drèze, "There is an urgent need for safeguards against unfair discontinuation of social benefits," *The Indian Express*, 20 April 2021, https://indianexpress.com/article/opinion/columns/aadhaar-linking-public-welfare-schemes-pds-system-7280621.

widows living alone, with fingerprint recognition problems," were some of the most vulnerable.[16]

Such problems are also tied to historical exclusion. Rather than sweeping away clunky, error-prone, paper-based systems as is often claimed, biometric systems are frequently layered upon older identification programs.[17] To enroll in the Aadhaar program, as Sriraman notes, one typically needs to provide documentation satisfying proof of identity and address, which reinforces "the continued relevance of existing paper-based ID documents."[18] While humanitarian and aid organizations may not place the same documentary demands when registering beneficiaries, their systems have become key gateways through which assistance is accessed, making exclusion especially critical.[19]

Foundational,[20] national Big ID programs also reproduce problems of statelessness and marginalization. Manby notes that "a state-backed foundational identity register for adults will almost inevitably make distinctions based on legal status in the country, between citizens and non-citizens."[21]

This also has implications for financial inclusion. By facilitating auditable and traceable digital transactions and fulfilling Know Your Customer (KYC) and Customer Due Diligence (CDD) obligations,[22] digital identity systems are touted as a way to provide financial services to the unbanked and those lacking formal financial histories.[23] Yet, as digital identity systems become increasingly central to financial transactions and the infrastructures underpinning them, those lacking official credentials can be blocked from accessing key services, including SIM registration and mobile money transactions–

---

[16] Jean Drèze, Nazar Khalid, Reetika Khera, and Anmmol Somanchi, "Food Security in Jharkhand: Pain without Gain," *Economic and Political Weekly* 52, no. 50 (2017): 54.
[17] Keren Weitzberg, "Biometrics, race making, and white exceptionalism: The controversy over universal fingerprinting in Kenya," *The Journal of African History* 61, no. 1 (2020): 23-43.
[18] Tarangini Sriraman, *In Pursuit of Proof: A History of Identification Documents in India* (Oxford University Press, 2018), 228.
[19] "Yemen crisis: UN partially suspends food aid," *BBC News*, 21 June 2019, https://www.bbc.com/news/world-middle-east-48716258.
[20] Foundational identity systems are civil registers, national identification databases, and population registration systems that are created to provide identification to the general population for a wide variety of transactions. In contrast, functional identity systems manage identification, authentication, and authorization for specific sectors or use cases, such as voting, taxation, social protection, or travel.
[21] Bronwen Manby, "The Sustainable Development Goals and 'legal identity for all': 'First, do no harm'." *World Development* 139 (2021): 7.
[22] KYC and CDD are global regulatory obligations guided by the Financial Action Task Force (FATF). They require financial institutions to do background checks on customers, verifying their identity and assessing their risk profile, among other measures, to tackle money laundering, terrorism, and proliferation financing.
[23] Alan Gelb and Caroline Decker, "Cash at your fingertips: Biometric technology for transfers in developing countries," *Review of Policy Research* 29, no. 1 (2012): 91-117; and "Biometrics and financial inclusion," FSD Kenya, 2 August 2019, https://fsdafrica.org/publication/biometrics-and-financial-inclusion.

challenges exacerbated by the emergence of super apps (discussed below). In addition, there is the risk that biometric systems and centralized information-sharing platforms can enable predatory forms of financialization, such as high-interest mobile micro-lending and data-driven credit scoring, leading in turn to financial exclusion.[24]

Big ID models, which centralize data and have limited options for end-user control and agency, are currently undergoing a radical transformation. Increasingly subject to criticism for data breaches, exclusion, and privacy harms, Big ID is facing a growing public relations crisis, as evidenced by recent controversies in Bangladesh and Afghanistan.[25] Such controversies have spurred an interest in decentralized digital identity models, as we discuss in the next section.

Self-sovereign imaginaries and decentralized identity

Unlike "Big ID," decentralized models for digital identity seek to remove the reliance on centralized parties by empowering users to control and manage their own identity data. With the advent of blockchain technology in particular, the notion of self-sovereign identity (SSI) has emerged as a popular manifestation of the decentralized digital identity model. A libertarian ideology underpins the blockchain and cryptocurrency movement.[26] In that spirit, proponents of SSI believe that individuals have the right to a digital identity that does not rely on third parties such as the state or another central authority.[27] Cheesman explains: "Just as Bitcoin facilitates pseudonymous inter-national exchanges outside the mechanisms of banks and other centralised financial authorities,

---

[24] Kevin P. Donovan and Aaron K. Martin, "The rise of African SIM registration: The emerging dynamics of regulatory change." *First Monday* 19, nos. 2-3 (February 2014), https://firstmonday.org/ojs/index.php/fm/article/view/4351/3820; Aaron Martin and Linnet Taylor, "Exclusion and inclusion in identification: Regulation, displacement and data justice," *Information Technology for Development* 27, no. 1 (2021): 50-66; Keith Breckenridge, "The global ambitions of the biometric anti-bank: Net1, lockin and the technologies of African financialisation," in *Ownership and Governance of Companies*, pp. 103-128 (Routledge, 2021); and https://www.cgap.org/blog/rethinking-consumer-protection-responsible-digital-finance-ecosystem.

[25] Human Rights Watch (HRW), "UN Shared Rohingya Data Without Informed Consent," HRW News, 15 June 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent; and Katja L. Jacobsen and Karl Steinacker, "Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered," Peace Research Institute Oslo (PRIO) (blog), 26 August 2021, https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered.

[26] Will Gottsegen, "Crypto's Core Values Are Running Headfirst Into Reality," *The Atlantic*, 9 September 2022, https://www.theatlantic.com/technology/archive/2022/09/crypto-technology-government-regulation/67137; Greg Ip, "Crypto Meltdown Exposes Hollowness of Its Libertarian Promise - WSJ," *Wall Street Journal*, 18 May 2022, https://www.wsj.com/articles/crypto-meltdown-exposes-hollowness-of-its-libertarian-promise-11652875201; and Georgia Frances King, "The Venn Diagram between Libertarians and Crypto Bros Is so Close It's Basically a Circle," *Quartz*, 23 May 2018, https://qz.com/1284178/almost-half-of-cryptocurrency-and-bitcoin-bros-identify-as-libertarian.

[27] Alexandra Giannopoulou and Fennie Wang, "Self-sovereign identity," *Internet Policy Review* 10, no. 2 (2021): 1-10.

libertarian SSI proponents suggest that blockchain will de-centre powerful authorities and intermediaries in digital identification and put the user in a position of greater power."[28] As we discuss below, however, ostensibly decentralized models rarely resolve the power asymmetries between users and identifying parties.

A key component of decentralized models is the digital wallet, where users can store their identity credentials (in the absence of a central database). Digital wallets "follow a variety of models, standards, and institutional and infrastructural arrangements, including but not limited to SSI," as Cheesman points out.[29] They do not require the use of blockchain, nor are they necessarily decentralized: "Among digital wallet projects that use blockchain, some propose a radical alternative to traditional currencies and identity management systems, but some do not–indeed, some of the most significant wallet initiatives are government led."[30] It must also be stressed that decentralized digital identity models still exhibit certain features of centralization, namely a reliance on what is currently a relatively small number of SSI technology providers and expertise. They also depend on centralized app stores, which may be subject to the influence of states and have already demonstrated a willingness to block access to certain applications, including wallets.[31]

In June 2021, the European Commission gave a boost to decentralized digital identity technologies by setting out plans for the future of pan-European identity management in eIDAS (electronic Identification, Authentic, and trust Services) 2.0. According to the promise of eIDAS 2.0, every EU member state will make a digital identity wallet available to any citizen who wants one by 2023. In the words of President of the European Commission Ursula von der Leyen, the vision is a "secure European e-Identity…that any citizen can use anywhere in Europe… a technology where we can control ourselves what data and how data is used."[32]

---

[28] Margie Cheesman, "Self-sovereignty for refugees? The contested horizons of digital identity," *Geopolitics* 27, no. 1 (2022): 140.

[29] Margie Cheesman, *Digital Wallets and Migration Policy: A Critical Intersection*, DoT.Mig In Brief, Migration Strategy Group on International Cooperation and Development (Bertelsmaan Stiftung, the German Marshall Fund of the United States (GMF), and the Robert Bosch Stiftung, June 2022), 16, https://www.bosch-stiftung.de/en/publication/digital-wallets-and-migration-policy-critical-intersection.

[30] *Ibid*, 16.

[31] Vignesh Karunanidhi, "Apple Blocks Coinbase Wallet Release on IOS," *Watcher Guru* (blog). 1 December 2022, https://watcher.guru/news/apple-blocks-coinbase-wallet-release-on-ios; Cate Cadell, "Apple Says It Is Removing VPN Services from China App Store," *Reuters,* 29 July 2017, sec. Media and Telecoms, https://www.reuters.com/article/us-china-apple-vpn-idUSKBN1AE0BQ.

[32] Ursula von der Leyen, "State of the Union Address," (transcript of speech delivered at the European Commission Plenary, Brussels, 16 September 2020), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

The EU's digital wallet initiative is explicitly intended to empower individuals. However, its emphasis on citizenship already suggests a lack of consideration for irregular migrants and non-citizens. In addition, the design is inherently exclusionary through its technological dependencies. Though intended to decentralize control over identity documents and empower the wallet holder, the proposed approach has been critiqued by the civil society group EDRi (European Digital Rights) for "lead[ing] us straight into surveillance capitalism."[33] As their analysis highlights, relying parties, including private companies, can check the credentials and attributes contained in the proposed wallet without any complementary regulation to limit the abuse of said data for tracking, profiling, targeting, or excluding a relying party from the system.

The design is also exclusionary for its reliance on users to both own a smartphone and have the technological capability to manage a digital wallet. Indeed, the Organisation for Economic Co-operation and Development (OECD) notes that just 75 percent of individuals in the EU used a mobile phone or smartphone to connect to the Internet in 2018, up from 65 percent just two years earlier.[34] A digital identity initiative that relies on smartphone ownership or access will only increase marginalization and exclusion, particularly of lower-income and vulnerable individuals–as is further elaborated in the discussion on super apps below. Furthermore, these systems have not been designed with vulnerable populations in mind, such as the poor, elderly, or migrants. They may fail to address, as Cheesman notes, "the segregation of refugees from mainstream financial instruments, markets, and identification systems."[35]

The European Commission's digital identity proposals are also significant because of the "Brussels effect"[36]–the international standard-setting and benchmarking of the bloc's policy and regulatory frameworks. Efforts to develop digital wallets are also underway outside the EU. The World Bank's ID4D 2021 Annual Report points to increased interest in "personal data wallets that offer alternative approaches to verifying identities."[37] However, there are widespread concerns about the use of complex technology systems in resource-constrained contexts. As Manby notes in reference to increased investment

[33] Thomas Lohninger, "Orwell's Wallet: European electronic identity system leads us straight into surveillance capitalism," EDRi (European Digital Rights), 2 February 2022, https://edri.org/our-work/orwells-wallet-european-electronic-identity-system-leads-us-straight-into-surveillance-capitalism; and EDRi and Epicenter.works, *eIDAS Policy Paper*, 25 January 2025, https://epicenter.works/document/3865.
[34] Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2020* (Paris: OECD Publishing, 27 November 2020), https://doi.org/10.1787/bb167041-en.
[35] Cheesman, *Digital Wallets and Migration Policy*, 16.
[36] Anu Bradford, *The Brussels Effect: How the European Union rules the world* (Oxford University Press, USA, 2020).
[37] World Bank, *ID4D and G2Px Annual Report 2021* (Washington DC, 2021), https://id4d.worldbank.org/annual-reports.

in biometric identification systems, these have "greatly increased up-front costs, for uncertain long-term benefits." At the same time, ID4Africa's survey of African identity authorities highlights how "vendor lock-in is the biggest cause of dissatisfaction" with the identity technology sector.[38] Despite data portability and interoperability commitments, digital wallets are inherently complex, requiring significant investment and reliance on technology suppliers. This also has implications for users. If digital wallets were mandated for interactions with the state or at borders, consideration would have to be given to users' technological capacity, digital infrastructures, and the demographics of those with device access. Data from the mobile industry body GSMA shows that only 49 percent of people across Sub-Saharan Africa have a smartphone[39]–meaning that any smartphone-based digital wallet will exclude 51 percent of the population. Similarly, research conducted by the International Federation of the Red Cross into a pilot deployment of SSI wallets in Kenya showed that users struggled with the technological requirements. The research found that: "SSI is impractical because it requires users to have good internet connectivity and (for full functionality) smartphones, as well as high digital literacy."[40]

SSI or wallet-based approaches to digital identity are heavily influenced by individualistic, libertarian ideals and, in themselves, assume a technological solutionism to concerns around centralized control and the realization of individual agency. Originally designed for "digital natives" in resource-rich, digitally "mature" Global North countries, they prove to be exclusionary in practice.

Super apps: platformizing digital identity

In parallel to the emergence of self-sovereign identity models and the development of decentralized identity wallets, there has been an explosion of another class of smartphone applications known as "super apps." One study estimates that one in three of the world's population is a super app user.[41] An increasingly predominant feature of many Asian digital economies, apps like Tencent's WeChat in China or Gojek in Indonesia combine seemingly disparate services—including financial (e.g. payments)

---

[38] Manby, "The Sustainable Development Goals," 6; Chris Burt, "Vendor lock-in hindering African identity projects," *Biometric Update*, 13 June 2018, https://www.biometricupdate.com/201806/vendor-lock-in-hindering-african-identity-projects.

[39] GSMA, *The Mobile Economy: Sub-Saharan Africa, 2022* (2022), https://www.gsma.com/mobileeconomy/sub-saharan-africa.

[40] The International Federation of Red Cross and Red Crescent Societies (IFRC), International Center for Humanitarian Affairs (ICHA), and Kenya Red Cross, *Dignified Identities in Cash Assistance: Lessons Learnt from Kenya* (2022), https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

[41] Ryan De Joya, Strategy Lead, Media Group, Dentsu Singapore, "Demystifying Superapps: Lessons from Singapore," in *Dentsu 2021 Year in Review*, https://brands.dentsu.com/year-review-2021/demystifying-superapps-lessons-from-singapore.

and non-financial applications (e.g. commerce, transportation, social media, communication, and identity)—within a single interface.[42] In creating such an all-in-one app, these platforms have been able to amass considerable amounts of data on users, which can be shared across services, making them a key innovation for digital identification. If the legacy of Big ID is the centralization of identity data (especially people's biometrics) with state and international authorities as the hub, and the ideological response to Big ID is a form of technological minimalism and data decentralization represented by the self-sovereign identity movement, then super apps can be viewed as the re-centralization of digital identity via massive commercial tech platforms. This transformation has important implications for both surveillance and socioeconomic inclusion/exclusion.

The case of Tencent is particularly instructive. As Jia et al. have explored, Tencent has leveraged four interrelated corporate strategies–conglomeration, financialization, platformization, and infrastructuralization–to accrue considerable power in China's digital economy.[43] Its super app, WeChat, can be used as a means of official identification for accessing both online and offline government services in major urban areas across China, with plans underway to expand the system nationwide.[44] In fact, Chinese super apps like WeChat and its main rival Alipay (offered by the Alibaba Group) operate in close partnership with the government and, in some cases, offer complimentary features, such as social-credit scoring and COVID health codes.[45] On these platforms, digital identities maybe accessible via a digital wallet feature within the app. For example, in countries like China, people are required to register on super apps with their real names and national ID numbers.[46] Perhaps more interestingly, irrespective of the inclusion of a digital wallet, these platforms can build rich, detailed profiles about their users because of the massive amounts of data generated through the use of the app, making them key actors in the digital identity ecosystem for years to come.

---

[42] Zennon Kapron, Joshua Chang, Mike McCaffrey, and Camilo Tellez-Merchán, "Improving Humanitarian Payments through Digital Innovation: Challenges and Opportunities, *Better than Cash Alliance,* August 2021: 72.

[43] Lianrui Jia, David B. Nieborg, and Thomas Poell, "On super apps and app stores: digital media logics in China's app economy". *Media, Culture & Society*, 44, no. 8 (2022): 1437–1453.

[44] Ayang Macdonald, "China to introduce digital ID cards nationwide," *Biometric Update*, 14 March 2022, https://www.biometricupdate.com/202203/china-to-introduce-digital-id-cards-nationwide.

[45] Xinmei Shen, "WeChat rolls out its own credit system nationwide, rivaling Alipay's Sesame Credit," *Abacus*, 5 June 2020, https://www.scmp.com/abacus/tech/article/3087781/wechat-rolls-out-its-own-credit-system-nationwide-rivaling-alipays; and Mia Zhong, "China's COVID Apps: A Primer," *DigiChina* (Stanford University), 14 July 2022, https://digichina.stanford.edu/work/chinas-covid-apps-a-primer.

[46] Zhong, "China's COVID Apps: A Primer."

The commercial success of super apps in Asia has inspired companies in other parts of the world to pursue similar strategies. Kenya's Safaricom, for example, is expanding its hugely successful mobile money app, M-Pesa, to include a wider range of services.[47] It is also trying to address concerns related to technological exclusion. Super app usage typically requires a smartphone and at least a basic (2G) connection for messaging and basic payment features. More advanced features necessitate faster connections (3G or better). While smartphones are still necessary for Safaricom's offering, its super app is available offline, allowing customers to use it and complete transactions without a data bundle or when disconnected from the network. Moreover, the app is "zero-rated,"[48] meaning it does not consume data to use, which should encourage uptake by low-income people.

Super apps also pose challenges in terms of further excluding the unbanked and undocumented from the digital economy. Because these apps often include payment mechanisms and access to financial service offerings, apps may require users to enter payment information and other financial details before transacting. People who cannot open a bank account (for example, migrants or refugees without proof of address) may therefore be limited in their use of super app features. Relatedly, people who lack forms of official identification may not be able to satisfy KYC/CDD regulations imposed on super apps unless regulators adopt a flexible approach. An example from India illustrates this concern. In February 2020, a Reserve Bank of India regulation would have canceled nearly 200 million digital wallets provided by super apps like Paytm (the market leader) that were deemed non-compliant. The Bank instead postponed enforcement and introduced a framework with transaction limits for "low-KYC" accounts to allow more time for super app accounts to comply with KYC rules. In this case, full KYC compliance involves remote authentication against Aadhaar–thus reinforcing the primacy of Big ID.[49]

While super apps have proven incredibly popular in countries in Asia and, to a lesser extent, Africa, strict data governance rules and antitrust laws in North America and Europe could impede their wider adoption in North America and Europe.[50] Nevertheless, this model is capturing the imaginations of tech companies like Twitter

[47] Paula Gilbert, "Safaricom launches M-Pesa 'super app'," *Connecting Africa*, 23 June 2021, https://www.connectingafrica.com/author.asp?section_id=761&doc_id=770425.
[48] Toussaint Nothias, "Access granted: Facebook's free basics in Africa," *Media, Culture & Society* 42, no. 3 (2020): 329-348; and Guy Thurston Hoskins, "Beyond 'zero sum': the case for context in regulating zero rating in the global South," *Internet Policy Review* 8, no. 1 (2019): 1-26.
[49] Zennon Kapron, Joshua Chang, Mike McCaffrey, and Camilo Tellez-Merchán, "Improving Humanitarian Payments through Digital Innovation: Challenges and Opportunities, *Better than Cash Alliance,* August 2021: 72-73.
[50] Gopi Billa, Zach Aron, and Mark Purowitz of Deloitte Consulting LLP, "Forecasting the Future of Super-Apps," *The Wall Street Journal,* 4 October 2022, https://deloitte.wsj.com/articles/forecasting-the-future-of-super-apps-01664903214.

and Meta, which are competing to build a dominant super app and have grand aspirations to route a range of services through these platforms.[51]

Recentering rights

Digital identity systems are not ends in themselves but are rather political in nature; as Whitley and Schoemaker argue, "they are developed by institutions as part of their pursuit of specific goals,"[52] with differing implications for both inclusion and rights.

In this article, we have illustrated how "Global North" countries with established identification regimes, often historically in the form of centralized Big ID schemes, are exploring alternatives, including so-called decentralized, wallet-based approaches. They are framing these efforts in the language of civic rights and empowerment, even as the systems they espouse are exclusive to those with technological access and capability, and often reinforce state demands for traditional credentials, if in digital form. At the same time, through their funding of development actors such as the World Bank, these same countries are supporting centralized digital identity systems for other parts of the world—a model that is increasingly unpalatable to citizens of the Global North.

In addition, despite a growing rhetorical commitment to decentralization, we see a continued dependence on state-issued identity credentials as the primary means of proving legal rights and entitlements–reinforcing the social contract between the state and citizen. In contrast, digital identity systems being developed by private sector providers, such as super app platforms, have little commitment or focus on inclusion and rights, and generate corporate value in the form of data generation and insights that enable the further commercialization of users.

Regardless of the approach taken, these new technological forms often serve to reinforce existing institutional arrangements, including state authority over the categorization of individuals, even where they are ostensibly designed to rebalance power in favor of individual autonomy. The more complex the technology, the more that problems of exclusion and power imbalances tend to be amplified. Such systems have significant implications for civil liberties and citizenship rights, particularly when they become effectively compulsory. As the transition to cashlessness has shown, the growing demand for digital payment platforms, such as credit cards or mobile wallets, has led to service denial and exclusion "from participation in the nation," particularly

---

[51] Barbara Ortutay, "Musk Has a 'Super App' Plan for Twitter. It's Super Vague," *Bloomberg UK,* 15 October 2022, https://www.bloomberg.com/news/articles/2022-10-15/musk-has-a-super-app-plan-for-twitter-it-s-super-vague.

[52] Edgar Whitley and Emrys Schoemaker, "On the sociopolitical configurations of digital identity principles," *Data & Policy* 4 (2022): 38. doi:10.1017/dap.2022.30.

amongst those “with precarious claims to citizenship”[53] and limited ability to produce the documents required by KYC and AML regulation. If the exercise of citizenship becomes increasingly mediated through digital identity technologies, we can expect to see novel forms of hierarchy emerge. Without attention to infrastructural, device-access, and capability requirements, a purely technological approach to the deployment of digital identity “solutions” may only magnify power asymmetries and patterns of exclusion, ultimately undermining rights.

Acknowledgments:

The authors would like to acknowledge Margie Cheesman and Paul Currion for their previous collaborations, Amos Doornbos for inspiring our recent thinking on these topics, and the Migration Strategy Group on International Cooperation and Development for their support.

Emrys Schoemaker is Research Director at Caribou Digital. He is affiliated with the Geneva Graduate Institute, Cornell Tech, and the London School of Economics.

Aaron Martin is an Assistant Professor at Maastricht University.

Keren Weitzberg is a Senior Lecturer in the School of Politics and International Relations and a Fellow at the Institute for Humanities and Social Sciences at Queen Mary University of London.

[53] Kate Coddington, "The slow violence of life without cash: borders, state restrictions, and exclusion in the UK and Australia," Geographical Review 109, no. 4 (2019): 527.