DIGITAL IDs

DIGITAL IDs
DIGITAL IDs

BY

MARDIYA SIBA YAHAYA and BONNITA NYAMWIRE

DIGITAL IDs
DIGITAL IDs
DIGITAL IDs
DIGITAL IDs

DIGITAL IDS

Mardiya Siba Yahaya and Bonnita Nyamwire

Interconnected and Moderated Bodies

Advocates for digital IDs claim they can provide legal identity to many who lack it, streamline government services, and reduce corruption.[1] Yet digital IDs inherit histories of structural inequalities and reproduce anxieties among the most marginalized.[2] Our contribution contends with these seemingly irreconcilable conditions by weaving together two key arguments. First, biometrics-based digital IDs are data that make people's bodies available for scrutiny at a distance. Second, digital IDs as aggregated datasets serve as a representation of the state, where logics of development and anti-corruption become the justification to collect more data in the pursuit of inclusion.

Digital IDs transform biometric information such as fingerprints, iris scans, and facial features into data. Approaching digital IDs as simultaneously standing in for data *and* the bodies of individuals reveals the conditions of surveillance that disproportionately target marginalized groups.[3] This data-as-bodies approach offers a situated perspective on the implications of the datafied state for the lives of women, gender and sexual minorities, and marginalized ethnic groups. For many among these groups, engaging with the datafied state brings up a range of anxieties — from losing access to systems and services because of failures in registration to the amplification of existing discrimination. Yet, there is also hope — hope to

1 World Bank Group, "Identification for Development: Strategic Framework."

2 Deborah Posel, "Race as Common Sense: Racial Classification in Twentieth-Century South Africa," *African Studies Review* 44, no. 2 (September 2001): 87–114, https://doi.org/10.2307/525576; Paul N. Edwards and Gabrielle Hecht, "History and the Technopolitics of Identity: The Case of Apartheid South Africa," *Journal of Southern African Studies* 36, no. 3 (September 2010): 619–39, https://doi.org/10.1080/03057070.2010.507568; Keith Breckenridge, "Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present," *The International Journal of African Historical Studies* 48, no. 1(2015): 148–150, http://dx.doi.org/10.1017/CBO9781139939546.

3 In this essay, we define marginalized as ethnic, racial, gender, sexual, and religious minorities. Gender and sexual minorities include women, queer, and non-conforming people.

finally achieve legal documentation of one's identity. In between this diversity of lived experiences, marginal citizens must navigate through existing relations of power to confront the limitations of the choices available to them.

Simultaneously, the aggregated datasets of unique digital IDs for all citizens serve as representations of the state; this representation is used in developmental efforts toward efficient and improved service delivery, achieving inclusivity, and tackling corruption.[4] In Zimbabwe, for example, after the Public Service Commission introduced a biometric system and ran an audit in 2020 in collaboration with the World Bank, they found 3,000 so-called ghost workers and removed them from the state's payroll.[5] However, signing up for biometric systems in various countries includes substantial information about and beyond those of the main registrant — the registrant's parents' name, parents' residence, or marriage details and certification,[6] to name a few. This data-as-state approach shows how national identification systems have historically provided states with the power to define acceptable citizen identities — shaping them into machine-readable humans.[7]

We focus on these two approaches to digital ID — data-as-bodies and data-as-state — to demonstrate how groups of peoples' socio-cultural, ethnic, gendered, and religious positionality affects how they engage with the state, how their data is used to inform service provision and delivery, and/or structurally discriminate against them. In our view, current datafied societies are embedded in regimes of monitoring and control, where data is used to make life-altering decisions for people whose data-as-bodies show up well before their actual selves.[8] Thus, throughout our essay, we trace the similarities and differences in historic and current ways identification exists and shows up in the lives of marginalized groups in Africa, the threats of control within datafied states, and a reflection that leaves more questions for further research.

4 Ranjit Singh, "Give Me a Database and I Will Raise the Nation-State," *South Asia: Journal of South Asian Studies* 42, no. 3 (May 2019): 501–18, https://doi.org/10.1080/00856401.2019.1602810.

5 Finbarr Toesland, "African Countries Embracing Biometrics, Digital IDs," *African Renewal*, February 2, 2021, https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids.

6 Quito Tsui and Teresa Perosa, "Digital IDs Rooted in Justice: Lived Experiences and Civil Society Advocacy towards Better Systems," *The Engine Room*, 2022, https://www.theengineroom.org/wp-content/uploads/2022/01/Engine-Room-Digital-ID-2022.pdf.

7 Janaki Srinivasan and Aditya Johri, "Creating Machine Readable Men: Legitimizing the 'Aadhaar' Mega e-Infrastructure Project in India," *In Proceedings of the Sixth International Conference on Information and Communication Technologies and Development: Full Papers* 1, 101–12. ICTD '13. New York, NY, USA: Association for Computing Machinery, 2013, https://doi.org/10.1145/2516604.2516625.

8 Jasbir K. Puar, "Jasbir Puar: Regimes of Surveillance," interview by Lewis West, *Cosmologics Magazine*, December 4, 2014, audio, https://writology.com/cosmologicsmagazine.

Designing "Machine Readable Humans": The Datafied State's Construction of Identities

Datafied states are the custodians of digital IDs. States have and continue to play the role of creators of "legitimized" identities, the implementers of systematic identification and artifacts that represent people's identities, the interpreters of the data collected, stored, and continuously developed through identification systems. In fact, citizen identities — right from the institutionalization of last names — have been designed as a mechanism to interface with the state.[9] Within and through these interfaces, human identities are converted into data.[10]

For example, during apartheid South Africa, the dompass was instituted in the Pass Laws Act of 1952, which required Black South Africans over 16 years old to carry a passbook at all times.[11] The dompass traced and identified whom a Black person belonged to. "Whom" did not refer to a person's clan, ethnic group, or family but to the white colonizer they worked for. Without the dompass, authorities could not verify whether the Black person had the *"right"* to access *"white"* spaces.[12] A similar requirement was created during the colonial era in Kenya, where indigenes were made to carry passes to access the new capital city of Nairobi.

Today, in our datafied society, whom we belong to in a transnational sense often refers to forms of belonging connected with countries and states based on ethnicity, place of birth, naturalization, or marriage. Yet, within the specific states, "whom" is also used to determine whether you have a claim to citizenship.

9 James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1998).

10 Silvia Masiero, "Digital Identity as Platform-Mediated Surveillance," *Big Data & Society* 10, no. 1 (January 2023): 1–5, https://doi.org/10.1177/20539517221135176.

11 "Dom Pass," Digital Innovation South Africa, March 31, 2021, https://disa.ukzn.ac.za/gandhi-luthuli-documentation-centre/dom-pass.

12 Paraphrased from a conversation between Mardiya with a South African acquaintance, while researching histories of IDs.

IDs represent claims to legitimately access certain services, privileges, and liberties. Based on the type of identification document one possesses, the level of available civic services and liberties ranges from high to none.[13] In each case, the state holds the power to interpret the data provided through each identification document or number at their discretion. This also means that when someone does not have access to a legal identity, their freedom of movement and access to basic services is blocked. This is the reality of Nubians and double-registered people in Kenya,[14] as well as refugees in Ethiopia who have faced technical barriers while registering for digital IDs.[15]

In 2018, the government of Kenya enforced the National Integrated Identity Management Scheme, requiring all citizens to register through a biometric identity system which they claimed to be a single point of truth.[16] In March 2023, the government of Kenya relaunched another system, the Unique Personal Identifier (UPI), to register all newborn babies and deaths in the country. The government used the UPI for school registrations, linked to citizens' "identification card, PIN number, National Health Insurance Fund, and Kenya Revenue Authority, as well as identify the individuals in life and in death." [17]

The goal of the UPI, according to the government, was to provide accurate insight and data on the country's population. Similarly, over the recent months in Tunisia, the government has rolled out a series of digital IDs including biometric travel documentations and the mobile ID or an e-identity (e-houwiya) that enables citizens to access government services.[18] Both governments argue that they need to create legible citizens to govern appropriately. At the same time, the Tunisian government argues that biometric identification and IDs need to be implemented by 2024 to fulfill the international civil aviation organizations' mandate for machine-readable

13 Ranjit Singh and Steven J. Jackson, "Seeing Like an Infrastructure: Low-Resolution Citizens and the Aadhaar Identification Project," *Proceedings of the ACM on Human-Computer Interaction* 5, no. CSCW2 (October 2021): 315:1–315:26, https://doi.org/10.1145/3476056.

14 UC Berkeley International Human Rights Law Clinic and Haki Na Sheria Initiative, "Digital Identity and the Legal Obligation to Conduct a Human Rights Impact Assessment in Kenya," April 2023, http://citizenshiprightsafrica.org/wp-content/uploads/HSI-UCB-Digital-ID-HR-impact-assessments-2023.pdf.

15 Zara Rahman and Sara Baker, "Digital ID in Ethiopian Refugee Camps: A Case Study," *The Engine Room*, 2019, https://www.digitalid.theengineroom.org.

16 Puar, "Regimes of Surveillance."

17 "Government Set to Launch Personal Identifier Portal," *Kenya News*, February 16, 2023, https://www.kenyanews.go.ke/government-set-to-launch-personal-identifier-portal/.

18 Chérif El Kadhi, "Tunisia's Digitization Programs Threaten the Privacy of Millions," *Access Now*, April 27, 2023, https://www.accessnow.org/tunisias-digitization-programs-threaten-the-privacy-of-millions/.

documents. Both the UPI and e-houwiya, like many digital IDs, are required to verify citizens' eligibility for state services, including verifying financial compensation, linking the IDs to other documents such as the national ID and passports. These cases demonstrate that datafied states seek to create interoperable systems to expand legibility *and* machine-readable citizens that can be known from a distance.

Within the datafied state, documentation, numbers, codes, and artifacts created to legitimize a person's belonging to a specific territory and access to services represent machine-readable humans. However, for citizens' bodies to be accessible to the state in ways that make them legible, identities must be crafted along certain parameters determined by governing institutions. The dompass existed to restrict free movement of Black South Africans during apartheid, which meant that the government crafted their identity along the parameters of race.[19] A person's race ultimately determined their interaction with the state and access to public spaces and services. In the datafied state, for humans to be machine-readable, their expressions, complexities, and realities must be limited to specific points, often a patriarchal reconstruction of gendered bodies, colonial demarcation of ethnicity, language, belonging, and ability. The power to be the creator, arbitrator, custodian, and interpreter of people's lives through digital IDs enables the state to have the discretion of what is considered legitimate identity or form of belonging versus illegitimate.

The case of Kenya and Nubians being denied identification has provided a clear case of states' power in determining belonging. The process requires people to provide certain forms of documentation or human verification that may not be available to them in the first place.

19 Posel, "Race as Common Sense."

Recognizable identities created at the state's disposition reinforce violence against minoritized genders. Within most states mentioned throughout this essay, non-conforming gender identities are criminalized. As we will explore further in the next section, the state's role in determining and controlling how people express their complex and fluid identity is enacted through the datafication of the body where a machine-readable human must be quantifiable in patriarchally acceptable ways. Meanwhile, the construction of the datafied body tends to follow the "traditional Western view of personhood as rationality"[20] that encodes people's interconnected, complex, and evolving lives into a set of scientific and mathematical formulas. States echo a logic that claims that their identification systems provide a single point of truth, often at the expense of minoritized groups. Such logic becomes harmful when the lives and identities of people are interconnected, making it possible to disproportionately target entire communities through automated systems that produce generalizations[21] and reconfigure violence and dehumanization.

Monitoring and Control: Cases of Surveillance Within Datafied States in Africa

In March 2022, a Ugandan queer activist based in South Africa stated in a video that she was advised that if she arrives at the Entebbe airport, she will be arrested immediately. While the video was a call to action to picket the Ugandan embassy in Pretoria against legalizing homophobic violence, the activist's story particularly emphasized a version of state surveillance. The Ugandan state is able to take action against the activist because it can identify through her machine-readable documents that she is part of and supports

20 Sabelo Mhlambi, "From Rationality to Relationality: Ubuntu as an Ethical and Human Rights Framework for Artificial Intelligence Governance," *Carr Center Discussion Paper Series*, no. 2020-009 (July 2020), https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial,2020).

21 Mhlambi, "From Rationality to Relationality."

a criminalized social group. Surveillance and exclusion are part of the architecture of digital identity platforms.[22] The state's ability to provide databases and information that enable profiling and policing with interoperability creates the possibility for surveillance.

Surveillance through interoperability[23] in the operationalization of digital ID systems is evident in the case of Ethiopian refugees who were miscategorized when they were initially registered and were later unable to register for a digital ID due to discrepancies in the system.[24] In Kenya, internally displaced persons who were affected by a severe drought in Northern Kenya that occurred at the same time as the Somali civil war[25] experienced the implications of surveillance when they attempted to register for a national ID, only to find out they had been categorized as refugees, blocking them from accessing national ID cards. Such errors affected multiple communities, and the lack of nuance based on "rationality"[26] restricted access to services for refugees and internally displaced persons.

Surveillance is also organized through social norms, categorizations of acceptable and unacceptable persons or identities and narrative shaping. It "uses such hegemonic norms and narratives to design multiple separations of people into normal/abnormal, good/evil, ally/enemy."[27] In creating these separations, Muslims, ethnic minorities such as Nubians, refugees, and double-registered people, are made[28] foreign by the system. Here Pumla Dineo Gqola points out that identity is performed across boundaries of difference,[29] and people such as educators and social workers who came to represent safe spaces or support the inclusive social development of marginalized groups, become the ones who facilitate monitoring and violence against the communities they are supposed to protect.

22 Masiero, "Digital Identity as Platform-Mediated Surveillance."

23 "Government to Launch Personal Identifier Portal."

24 Zara Rahman and Sara Baker, "Digital ID in Ethiopian Refugee Camps: A Case Study," The Engine Room, 2019, https://www.digitalid.theengineroom.org.

25 "When ID Leaves You Without Identity: The Case of Double Registration in Kenya," *Privacy International*, December 20, 2021, https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya; UC Berkeley International Human Rights Law Clinic and Haki Na Sheria Initiative, "Digital Identity and the Legal Obligation to Conduct a Human Rights Impact Assessment in Kenya," April 2023, http://citizenshiprightsafrica.org/wp-content/uploads/HSI-UCB-Digital-ID-HR-impact-assessments-2023.pdf.

26 Mhlambi, "From Rationality to Relationality."

27 Mardiya Siba Yahaya, "What Can Digital Surveillance Teach Us about Online Gender-Based Violence?" GenderIT.org, November 1, 2021, https://genderit.org/feminist-talk/what-can-digital-surveillance-teach-us-about-online-gender-based-violence.

28 Pumla Dineo Gqola, *Female Fear Factory: Gender and Patriarchy Under Racial Capitalism* (Nigeria: Cassava Republic Press, 2022).

Within various African countries, SIM card registrations provide other avenues for increased data collection and surveillance. While SIM cards have long represented a form of digital identity, SIM registration has become an invasive area where the state, through telecommunication companies, promotes the surveillance of its citizens. For example in Uganda, for an individual to register for a SIM card they must present an original national identification card, passport or number, which must be verified by the SIM card-selling officer using a two-step authentication process. In addition, the telecom operator must obtain the photograph of the SIM card applicant. This same situation applies to Nigeria, Ghana, Namibia, and most recently Zambia. Such registration requirements exclude many marginalized groups such as ethnic minorities or migrant workers, and women without ID proof such as birth certificates, needed to obtain a digital ID, which has become mandatory to get a SIM card. Simultaneously, without structural safeguards, the datafied state creates additional databases linking citizens to their mobile number and interpersonal transactions, loosening the boundaries between tracking, identifying, monitoring, screening, and tabulating.

The increased datafication of the people's lives and bodies through SIM cards widens the bounds of how people become legible within a datafied state. The state logic that datafication of people through digitalization will provide single points of truths, including addressing corruption and streamlining service delivery, operates based on conceptions that governance requires people to be made recognizable and legible. However, the implications of surveillance within the datafied state are not evenly distributed. For instance, a gender and sexual minority or migrant worker whose body has been categorized as a threat enforced through public policies and legislature is more likely to be targeted through these interoperable systems that monitor, screen, and analyze their day-to-day interactions. If a person's SIM

29 David W. Tarbet, Michel Foucoult, and Alan Sheridan, "Discipline and Punish: The Birth of the Prison," *Eighteenth Century Studies* 11, no. 4 (January 1978): 509, https://doi.org/10.2307/2737970.

card is linked to their digital ID, biometrics, mobile money transactions, and internet activity, it creates multiple avenues for datafied states to enact harm. Preemptive surveillance to track and shape what a person will do in the future forces ethnic, racial, religious, gender, and sexual minorities to constantly navigate between the choices of enrolling in digital ID systems or opting out to their detriment. Yet by merely engaging in life, social and civic interactions within datafied states and societies, people's data and information is collated, tabulated, tracked and screened, regardless.

Reflecting on the Complicated Fluidity of Individual Autonomy Versus Communal Data

Individual identity, as argued throughout this essay, is moderated by the state. Simultaneously, states make decisions across differences and similarities in how certain groups perform their identities. Data gathered on one person may produce insights on people whose attributes fall into similar categories. For example, when a person is registering for a digital ID, they have to provide verifiable information on their parents and other family members. Similarly, the case of the Ugandan activist provides insights into how decisions are rarely individualized, and made based on social group identities. At the same time, automated immigration decision-making is often based on what people of certain races, locations, and identity "might do." This includes predefined problematic assumptions such as that Muslims are more likely to be engaged in violence extremism or that someone from the Global South is more of an immigration risk than someone from the Global North. All these decisions are encoded in policy, structural designs, and cultural hegemonies reproduced through identification systems and technologies.

While the previous sections have illustrated the differences between the data-as-bodies approach and the data-as-state approach in understanding the politics of digital IDs, we conclude with a reflection of a deeper similarity between them. Both these approaches are fundamentally grounded in a relational view to datafication.[30] This relational view opens up questions such as — what does one's data reveal about a community of people? How does that information create tensions between the individual and the community? How does one tackle a situation where an individual may have consented to data collection, but their data implicates other people "like them" who had no part in that process? What does this mean for a person's individual identity and their right to privacy?

Many African philosophies and practices have evidenced that human engagement, personhood and lives are representations of communities, and eventually flourish through such forms of solidarities. While we do not have specific answers to these questions, they enable us to draw the tensions between autonomy and belonging in the context of datafication. The opposite can also be true, where such relationality provides an opportunity to manifest autonomy through belonging in a participatory approach to designing inclusive data systems. We critique individuation through datafication as a continuation of a history of harms against marginal communities and perpetuation of ongoing forms of violence against them. The simplest way to challenge this process is to ask ourselves whether single points of truths can ever be an accurate approach to govern our complex and fluid communal lives.

30 Salomé Viljoen, "A Relational Theory of Data Governance," *Yale Law Journal* 131, no. 2 (November 2021): 370–781, https://doi.org/10.2139/ssrn.3727562.