"DNA AND GPS COORDINATES, PLEASE": A KENYAN CASE STUDY ON THE RISKS OF DIGITAL IDENTIFICATION SYSTEMS

ANNA AGATHIS*

*JD, New York University School of Law, 2026. I would like to sincerely thank Professor Kevin Davis for seeing this project through its many iterations and providing invaluable guidance on transnational law and development as well as Professor Angelina Fischer for her insight on digital infrastructure and human rights law. Finally, I would like to thank all the editors of the Journal of International Law & Politics for their comments and revisions and my family and friends for their support.

I. INTRODUCTION

In 2018, the Kenyan government quietly swept into law an advanced digital identification program that would mandate the collection of biometric information, DNA, and GPS coordinates within Statute Law (Miscellaneous Amendment) Act No. 18 of 2018.[1] The Kenyan digital identification program, which is now in its third iteration, has been at the center of multiple legal controversies. Originally intended as a method of increasing electoral legitimacy,[2] the ID program instituted nationwide collection of biometric data,[3] implicating rights of anti-discrimination and privacy.[4] As a result, a cadre of non-governmental organizations pursued litigation both inside and outside of Kenya. The first arm of the litigation strategy pressed straight to the Kenyan government through the Constitution while the second

1. The Statute Law (Miscellaneous Amendments) Act 2018, No. 18 Cap. 107 § 9A, KENYA GAZETTE SUPPLEMENT NO. 161 [hereinafter, Statute Law]. The High Court at Nairobi analyzed the constitutionality of the National Integrated Identity Management System. The final decision came out in 2021 following the government's enactment of a data privacy law. The NIIMS project was preceded by the Kenyan Integrated Elections Management System, or Huduma Namba, *see* Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) (2020) KEHC 8772 (KLR) at ¶ 23 – 26 (finding violations of the right to privacy and freedom from discrimination) and has been succeeded by *Maisha Namba, see Haki na Sheria Initiative v Attorney General & 4 others* [2024] KEHC 10021 (KLR), ¶ 56 (setting aside the conservatory order which halted the implementation of Maisha Namba and effectively dismissing the constitutional claims).

2. The IEBC uses biometric data through the BVR system to register voters. Voter Registration System INDEP. ELECTORAL AND BOUNDARIES COMM'N, https://www.iebc.or.ke/voting/?bvr.

3. *See* Rose Morero, *In Kenya's 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand*, CARNEGIE ENDOWMENT FOR INT'L PEACE (2022) (providing an overview of the recent history of digital identification systems in Kenya).

4. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) (2020) KEHC 8772 (KLR) at ¶ 23 – 26 [hereinafter Nubian Rights Forum].

circuitously reached for corporate accountability under the French Corporate Due Diligence Law.[5]

This note brings to light the normative arguments around digital infrastructure projects in the Global South through the study of the dual litigation strategy against the Kenyan government and its corporate supplier. In exploring these normative arguments, I posit that digital infrastructure itself is an ethically neutral technology that can be manipulated to advance developmental goals as much as disrupt human rights ones. Digital infrastructure can become a weapon of an authoritarian regime or a tool for enfranchisement depending on the goals of those wielding it, the protective regulatory structures in place, and the socio-political environment in which it is employed. The dual litigation strategy elucidates how each of these variables can distort digital infrastructure projects and where actors may intervene to reorient them.

The dual litigation also carries stakes beyond those of data regulation. It juxtaposes two approaches to human rights advocacy – state responsibility and corporate accountability.[6] The former concerns a state's actions toward its own people, while the latter is a trending approach to tackle human rights abuses in the Global South by largely extractive European actors.[7] State responsibility is explored through the constitutional claims laid against the Kenyan government. However, the corporate liability approach, though targeting European actors, still affects non-European states: increased corporate standards in Europe are foisted onto developing states through contractual relationships and bilateral agreements. While the change in standards is only formally affecting European corporations, the result is that those obtaining their services must also meet the appropriate standards. This method of standard setting was particularly controversial in the context of the CSDDD where discussions were cabined to European actors and excluded the nations who would bear the lion's share of

5. Loi 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre [Law 2017-399 of March 27, 2017 on the Duty of Vigilance of Parent Companies and Contractors], Journal Officiel de la République Française [J.O.] [Official Gazette of France], March 28, 2017 [hereinafter Devoir de vigilance]. *Supra* at 4.

6. For further discussion on the role of the colonial legacy in international law, *see* Antony Anghie, *Rethinking International Law: A TWAIL Retrospective*, 34 EUR. J. OF INT'L. L. 1, 7 (2023), https://doi.org/10.1093/ejil/chad005.

7. This trend is aptly demonstrated by the emergence of the Corporate Sustainability Due Diligence Directive (CSDDD). Council Directive 2024/1760, 2024 O.J. (E.U.).

compliance costs.[8] I argue that the litigation strategy at issue here is notably different as a French NGO teamed up with two Kenyan NGOs, but that the risks for non-European states when standards are raised abroad are deeply relevant.

Allowing European standards to unilaterally influence the procurement contracts with African states is contentious because of its similarity to the ethos of the civilizing mission.[9] The goal then becomes finding a line between utter neglect of the ills produced by corporations abroad and cognizance of the condescension in constructing a system meant to protect foreign nations without involving the most relevant actors – governments in the Global South. Therein lies the strength of this litigation strategy: its *dual* ability to confront the Kenyan government's constitutional duty and engage a corporation at risk of civil liability for its extraterritorial harm. Furthermore, the siloing of parties is valuable in the context of corruption allegations, as occurred in the Kenyan case. When the government's motives are suspect, the NGOs and attorneys who pursued this litigation operate as a secondary means of serving the public interest.

In taking on a comparative analysis of these two litigation strategies, I interrogate the root causes of the human rights risks associated with digital ID, and in turn, how domestic constitutional law and transnational corporate liability law each address the unique risks attached to digital ID. Although digital ID systems have long been presented as a panacea to developing countries who seek technology to accelerate development, this account considers the less told story in which an individual's most personal information and their access to basic services loom in the balance.

A. *Overview*

The note begins with a brief overview of digital identification systems and their capacity to elevate or subjugate fundamental rights. In its basic form, identification is predicated on one's civil registration collected and maintained by the government. Registration, or the inputting of information relating to an individual, includes events like birth, marriage, and death. Identification then uses the inputted data from registration to ensure one's identity. Traditional forms of civil registration and identification are compared to newer approaches in which biometric data is inputted at registration and subsequent identification

---

8. *See* Kevin Davis, Roy Germano & Lauren E. May, *Did the Global South Have Their Say on E.U. Supply Chain Regulation?*, 32 IND. J. GLOB. LEGAL STUD. 39 (2024).

9. It advances a narrative that Europeans allegedly have superior ethics that they must impose on others for their own good.

enables financial functions like the opening of a bank account. The analysis acknowledges the power dynamics that allow civil registration and these "economic IDs" to serve as tools of enfranchisement in some cases and exclusion in others.

The second section traces the relationship between biometrics in voter registration, the predecessor to Kenya's digital ID, and political violence in Kenya. The violence arising out of the 2007 election represents the foundational cause for the implementation of a biometrics system. The section proceeds through the different stages of increased digitalization of identity data and its failure to resolve the political unrest. Eventually, the digitalization practices resulted in the creation of the first iteration of a wide-reaching digital identity technology, dubbed "KIEMS," which would be associated with the overturning of the 2017 election and subsequent political fallout.

In the third section, the constitutional claims brought to the High Court of Kenya by three Kenyan NGOs inform the normative debate around digital ID with a focus on the data privacy and human rights concerns. The Indian digital identification system, Aadhaar, is used to position the Kenyan ID system along the spectrum of digital ID practices through a comparative analysis. To appreciate the risks and ramifications in the Kenyan context, the ethnic division and the plight of Nubians is briefly addressed. Then the analysis returns to the political controversy around KIEMS to consider what implications persist in using the same hardware for NIIMS. Finally, the dissection of the case culminates in a deep discussion of the regulatory infrastructure and its failure to save the NIIMS project from itself.

The fourth section takes up the second arm of the litigation – the Duty of Vigilance claims in France – and considers the social and legal goals of targeting an invasive Kenyan governmental scheme through the supplier side. It begins by distinguishing the Duty of Vigilance from other due diligence programs for its forward-thinking capabilities and establishing its unique suitability for NIIMS. The discussion then explores the success of the mediation ordered through an analysis of IDEMIA's updated vigilance plan. The plan operates as both a prophylactic aimed at future litigation as well as a step toward advancing the discourse of corporate liability for human rights. The goals served by the mediation and updated plan are evaluated within the framework of the dual litigation strategy and the social implications of the cross-border litigation.

In the final section, the accomplishments of the litigation are reevaluated in light of the Kenyan government's institution of the newest digital ID system, Maisha Namba - a less intrusive but potentially harmful reformation of Huduma Namba (NIIMS). The analysis

considers the long-term effects of the entire litigation strategy, and the normative changes made to digital identification, constitutional activism, and corporate responsibility through these two cases.

B. *Digital ID Systems as Development Solutions*

Understanding the litigation against digital identification stakeholders requires first understanding the impetus behind such systems, and in the Global South, it is avowedly developmental. The World Bank provides the most comprehensive discussion of how to create registration systems for institutional development, dubbing the program "Identification for Development" or "ID4D."[10]

This note uses many concepts relating to identification system that require definitions as each refers to a distinct process within digital infrastructure. Digital infrastructure uses two separate processes – registration and identification – to verify one's identity. Registration refers to the creation of a unique identity record and the "issuing of credentials to allow people to assert that identity." In this discussion, identification is used to refer broadly to the composite processes of authentication and authorization, which include verification of attributes and confirmation or rejection that an individual is who they claim to be.[11]

1. *Identification Fundamentals*

Civil registration and vital statistics (CRVS) is the foundation of most national identification systems – its collection is considered a critical government function.[12] CRVS uses principal events like birth, marriage, and death to inform the civil registry, which is then used in verification practices. While CRVS is not itself an identification practice, it is used to inform national identification systems. In the upcoming discussion, CRVS references both the registration practice and the identification system it informs. National identification systems employ

---

10. *See Identification for Development*, WORLD BANK, https://id4d.worldbank.org/ (last visited Aug. 25, 2025).

11. Identity refers to the "characteristics that make a person unique in a given context." *Practioner's Guide: ID 101 Basic Concepts,* WORLD BANK, https://id4d.worldbank.org/guide/id-101-basic-concepts-0 (last visited Aug. 25, 2025). While many of these terms and definitions are borrowed from the World Bank ID4D materials, they are employed in a different capacity, meaning they do not have the same definitional relationships.

12. WORLD BANK, *GLOBAL CIVIL REGISTRATION AND VITAL STATISTICS: SCALING UP INVESTMENT PLAN 2014-2024* (May 28, 2014), https://www.worldbank.org/content/dam/Worldbank/document/HDN/Health/CRVSScaling-upoverview5-28-14web.pdf.

CRVS to generate and authenticate one's recorded legal identity and ensure access to essential services.[13]

Birth registration, the first component of CRVS, is considered a human right recognized by both the International Covenant on Civil and Political Rights and the Convention on the Rights of the Child because of the bearing it has on the freedom in one's life.[14] It is intimately tied to a bundle of fundamental civil, political, social, and economic rights. Death certificates, the second component of CRVS, prevent identity fraud and ensure the management of benefits and services to those who need it.[15]

While the World Bank calls CRVS "a fundamental function of governments," over a hundred developing countries lack the infrastructure to keep up with it.[16] At the heart of the CRVS problem is the failure of the administrative state to act on behalf of its population. The development and regulation of CRVS is an administrative duty within the control of the state, and the development benefits are incontrovertible. Yet, states still impede the functioning of CRVS and infringe the umbrella of rights tied to it. The failure to register an individual's birth can pose a lifelong burden on the individual, hindering movement, employment, electoral rights, property rights, and financial autonomy. CRVS, among other identification programs, can be jeopardized through preexisting practices, rules, or regulations that discriminate against marginalized communities and interfere with registration.[17] For those not registered at birth, the administrative burdens can be overwhelming or impossible, such as fees, transportation costs, or proof of

13. *Id.* Strictly speaking, one's identity exists regardless of recognition from the government, but it derives power from its legal recognition. By inputting one's characteristics into a government database and receiving unique credentials, each individual feeds into the system of knowledge production system wielded by the government. In return, their "legal identity" is generated.

14. *See* International Covenant on Civil and Political Rights art. 24, Mar. 23, 1973, 999 U.N.T.S. 171 (citing the right of every child "to be "registered immediately after birth"; *see* Convention on the Rights of the Child, art. 7 (Nov. 20, 1989), 1577 U.N.T.S. 3, 28 I.L.M. 1448 (1989) (entered into force 2 Sept. 2, 1990) (providing for the rights to registration after birth and to acquire a nationality).

15. CRVS refers broadly to the act of recording and documenting vital events in a person's life (including birth, marriage, divorce, adoption, and death). WORLD BANK AND WORLD HEALTH ORGANIZATION, GLOBAL CIVIL REGISTRATION AND VITAL STATISTICS SCALING UP INVESTMENT PLAN 2015 – 2024 (May 28, 2014). https://openknowledge.worldbank.org/server/api/core/bitstreams/371e85c6-e7f6-529b-b6f0-800267108692/content.

16. *Id.* at xii.

17. *Id.* at xii.

parents' citizenship.[18] The heightened risk for marginalized communities is a principal concern in both lawsuits at the center of this study.

2. *Economic Identity and (Dis)Enfranchisement*

The UN-Legal Identity Expert Group recommends that legal identity "be conferred by a legally recognized identification authority… linked to the civil registration system."[19] Legal identity should in turn allow citizens to access a myriad of other basic rights. "Economic" identity, a term employed by scholars at the Center for Human Rights and Global Justice at New York University School of Law (CHRGJ), is an alternative form of legal identification.[20] Economic IDs "enable paperless, cashless, remote, and data powered transactions." Aadhaar, the Indian digital ID used to facilitate transactions, is the quintessential form of such economic IDs.

While it aims to promote economic empowerment, economic identity – unlike traditional legal identification practices (e.g. CRVS) – does not always connect identification to the provision of fundamental rights discussed above.[21] This is primarily because economic IDs are used to determine and authenticate "uniqueness" and then approve a particular transaction, but the technology need not be linked to one's legal status. The primer by CHRGJ criticizes the new era of digital IDs' cognizant oblivion to "legal status" or "legal identity" as dooming the projects to the "underlying dynamics of social exclusion, economic inequality, and marginalization" that predate its existence.[22] The failure

18. *Id.* at 8.

19. CTR. FOR HUM. RTS. & GLOB. JUST., N.Y.U. SCH. OF L., PAVING A DIGITAL ROAD TO HELL? A PRIMER ON THE ROLE OF THE WORLD BANK AND GLOBAL NETWORKS IN PROMOTING DIGITAL ID, CENTER FOR HUMAN RIGHTS AND GLOBAL JUSTICE (June 2022), https://drive.google.com/file/d/1VOUre5pBGB2i9sjPc5gAAxq_xozijh9-/view [hereinafter CHRGJ]. U.N. Legal Identity Expert Grp., *United Nations Country Team: Operational Guidelines* 9, (May 2020), https://unstats.un.org/legal-identity-agenda/documents/UNCT-Guidelines.pdf.

20. *See* CHRGJ, *supra* note 19, at 47. CHRGJ notes that there has been a significant divergence from the lofty, rights-based agenda of the World Bank and the reality of the economic/transactional identification model. *Id.* For example, a recent project by the World Bank in South Africa delinks the unique identification number from any legal status or entitlement. *See* WORLD BANK, PROJECT APPRAISAL FOR THE WEST AFRICA UNIQUE IDENTIFICATION FOR REGIONAL INTEGRATION AND INCLUSION (WURI) PHASE 2 (Apr. 10, 2020), http://documents1.worldbank.org/curated/en/261151588384951057/pdf/Benin-Burkina-Faso-Togo-and-Niger-Second-Phase-of-West-Africa-Unique-Identification-for-Regional-Integration-and-Inclusion-WURI-Project.pdf.

21. CHRGJ, *supra* note 19, at 48.

22. *Id.* at 12.

to consider the rights tied to one's legal status and instead base legal identification on a single, unique characteristic silos the goal of legal enfranchisement from that of registration and identification. All should be wary of such siloing as the ultimate distortion of such identification practices was the tool employed in both the Nazi and Rwandan genocides, in which registration and identification without reference to legal rights were leveraged to perpetrate ethno-centrist violence.[23] However, that does not make identification a wholesale evil but rather a double-edged sword. Nor should the two be reduced to a "good" form of legal identity and a "bad" form of "registration." Rather, normative judgements on identity and identification can abound in both directions. The takeaway then is that identification is an "exercise of power," and therefore can be exploited.[24]

Even as the "new paradigm" of digital economic identity promotes financial development, it jeopardizes basic rights when one is excluded from government recognition.[25]An article by Jaap van der Straaten in response to the ID4D initiative pointed out the pattern of exclusion from identification systems in developing countries generally,[26] while the Special Rapporteur on Extreme Poverty and Human

---

23. *See, e.g.,* Timothy Longman, Identity Cards, Ethnic Self-Perception, and Genocide in Rwanda, in *Documenting Individual Identity: The Development of State Practices in the Modern World* 345 (Jane Caplan & John Torpey eds., Princeton Univ. Press 2001), http://www.jstor.org/stable/j.ctv301fxj (providing a global perspective on the dangers of identification programs by sharing real-life accounts). Caplan and Torpey emphasize how "bureaucratic processes of individual identification have been put to nightmarish use, the most notorious example being the Nazis' use of population registers and identification documents to track Jewish and other "undesirable" populations." *Id.* at 5. Timothy Longman, in his chapter, similarly examines the role of ethnic identity cards in the perpetuation of Rwandan genocide. *Id.* at 345-358.

24. CHRGJ, *supra* note 19, at 48.

25. *Id.* The argument advanced by CHRG is that the Bank employs the rhetoric of human rights language but does not carry out those considerations in practice. Natalie Brinham et al., *Locked in and Locked Out: The Impact of Digital Identity Systems on Rohingya Population*, INST. ON STATELESSNESS AND INCLUSION, Nov. 2020, at 18 https://files.institutesi.org/Locked_In_Locked_Out_The_Rohingya_Briefing_Paper.pdf. This briefing paper remarks on the responsible use of identity technology. The goal of such approaches is to "ensure the meaningful participation of beneficiaries and balance unequal power relations."

26. "83 ID systems in low income and lower- and upper middle-income countries for which coverage data were available in the Global Findex survey of 2017, there clearly is a coverage pattern that causes the poorest people to be left out from ID-systems the most," Jaap van der Straaten, *Identification for Development It Is Not. 'Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable'-A Review.*, SSRN ELECTRONIC J. 5 (2020), https://doi.org/10.13140/RG.2.2.19300.19841.

Rights, Philip Alston, has bemoaned digital ID's exclusive nature.[27] Without these rights-based impact assessments, the dangers of digital ID would continue to hide behind the rhetoric of its unqualified developmental capabilities.

Digital economic identity systems may further threaten human rights when identification is not linked to attributes like birth registration and citizenship that enable access to government services. Therefore, digital ID has the potential to not only inhibit development goals but can even serve as a means of formal exclusion.[28] Additional concerns arise as digital identification is leveraged in commercial contexts. In Kenya, the significant investment in biometric technology alone entrenched the technological solution despite the injury to privacy rights and reproach of its intrusive nature by the judicial branch.[29] Again, this is a complex narrative; on the one hand, digital IDs contribute to economic enfranchisement through banking and microfinance, but on the other, it brings governments to prematurely invest significant amounts of capital in unregulated technology before a risk assessment and regulatory scheme can be contemplated.

The developmental goals touted by the World Bank as well as the counter-narrative expressed by scholars and legal advocates represent two sides of the same coin. These two viewpoints explain how a lofty digital ID program meant to expand fundamental rights resulted in multi-pronged litigation by human rights organizations. In order to understand the political and economic decisions behind digital infrastructure projects, one must remember that digital identification is only one element in the vast pool of data flowing into the government's digital infrastructure, integrating information across sectors through interoperable information systems.[30] Governmental and non-governmental

---

27. Philip Alston (Special Rapporteur on Extreme Poverty and Hum. Rts.), *Digital Technology, Social Protection and Human Rights: Report*, U.N. Doc. A/74/493 (1 Oct. 1, 2019).

28. CHRGJ, *supra* note 19, at 3148.

29. As discussed in Parts 1 and 2, the NIIMS program was informed by the recommendation to use biometric technology solutions to increase electoral legitimacy. However, Part 3 explains that the Kenyan government still proceeded to create a new iteration of digital ID, Maisha Namba, based largely on biometrics that poses risks to data privacy.

30. Julia CLARK., GEORGINA MARIN., OYA PINAR ARDIC ALPER & GUILLERMO ALFONSO GALICIA RABADAN FOR WORLD BANK, DIGITAL PUBLIC INFRASTRUCTURE AND DEVELOPMENT: A WORLD BANK GROUP APPROACH. DIGITAL TRANSFORMATION WHITE PAPER, VOL. 1 (2025), https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf. The World Bank explains the different

actors have been making the move to forms of digital identification that include biometric information such as retina scans or fingerprints to facilitate quicker access and avoid allegations of fraud.[31] However, those new forms of ID are still linked to other databases of government information, including those tracking physical IDs. When digital IDs enter the scene, as is the case in Kenya, the database may link together all data on an individual, including financial and banking information, creating an intrusive portrait of the individual's life.[32]

Further complications occur when an individual provides their biometric data for one purpose, but the government expands the number of actors, both public and private, to whom that information may be accessible. In the case of Aadhaar, the Indian digital identification project, additional functions were stacked on top of basic government identification; as a result, the purely governmental project quickly morphed into a highly commercial one as well and raised even more privacy concerns.[33] As Aadhaar was much of the inspiration for NIIMS, it will

---

approaches to digital identification. A fragmented approach to digitalization has each sector building its own end-to-end digital services. The Bank notes the power of Digital Public Infrastructure (DPI) is its ability "to integrate into a variety of sector applications" when "sectors have a variety of digital systems, including digitized databases and registers, interoperable information systems…" DPI can only be realized, according to the World Bank, by having continuous coordination across government entities including: "including digital agencies, line ministries, and regulators; participation and collaboration of the private sector; and regular engagement with CSOs, the public, and other stakeholders."

31. *See* WORLD BANK GROUP, *A Primer on Biometrics For ID Systems* (2022), https://documents1.worldbank.org/curated/en/099025009302216641/pdf/P17159207bc5150a308b380001fc5e8e0ff.pdf. Hannah Quay de la Vallée, *Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives,* Blog Post, CTR. FOR DEMOCRACY AND TECH. (June 7, 2022). On the use of biometrics by non-governmental organizations, see Çağlar Açıkyıldız, Unique data, different values: Explaining variation in the use of biometrics by international humanitarian organizations, 15 *GLOBAL POLICY: NEXT GENERATION*, 502–515 (2024), https://doi.org/10.1111/1758-5899.13343.

32. CHRGJ, *supra* note 19*,* at 50.

33. For more on the "India stack," *see* Yan Carriere-Swallow, V. Haksar & Manasa Patnam. *India's Approach to Open Banking: Some Implications for Financial Inclusion*, IMF Working Paper No. 2021/052 (2021), https://doi.org/10.5089/9781513570686.001. Manveena Suri, *Aadhaar: India Supreme Court Upholds Controversial Biometric Database***,** CNN (Sept. 26, 2018), https://www.cnn.com/2018/09/26/asia/india-aadhaar-ruling-intl/index.html**.** Many concerns about Aadhaar were laid to bed after the Indian Court restricted its use, preventing Aadhaar from being mandatory for opening bank accounts, obtaining sim cards, or enrolling children in schools, Anuradha Shukla, *Aadhaar Must for New PAN Card*, ECONOMIC TIMES (June 19, 2025), https://economictimes.indiatimes.com/news/india/aadhaar-must-for-new-pan-card/articleshow/121938784.cms?from=mdr. Although there is question as to whether it is not

be studied as a means to comparatively analyze the risks of stacking in digital infrastructure.

Unlike its Indian predecessor, the Kenyan digital ID system incorporated biometrics to quell the loss of trust in the democratic process. Before NIIMS, there were two attempts to use biometric information to restore the legitimacy of electoral voting with significant problems. Despite the technology's failure to appease the political instability, the Kenyan government continued moving forward with a form of digital registration and identification that would be the most invasive to date. To understand the decision, the electoral politics of the preceding years are the most informative.

II. DIGITAL SOLUTIONS TO POLITICAL PROBLEMS

Throughout Kenya's recent history, the government has presented digital infrastructure as promoting accountability and increasing legitimacy amidst political turmoil. However, behind that façade has been a prolonged controversy around public corruption, political entrenchment, and government mistrust that has been exacerbated by the incorporation of digital ID. The Kenyan government went through multiple iterations of digital identification technologies but never alleviated the concerns largely rooted in normative criticism of digital identification technology.

A. *2007 Election Violence*

Kenya's fraught political history planted the seeds of digital ID's placative role. The past few election cycles in Kenya have raised the need for increased electoral transparency and legitimacy – a goal which digital ID seemed well suited for. In 2007, the incumbent president Mwai Kibaki – of the Kikuyu tribe – was challenged by Raila Odinga – a Luo.[34] The upset by Kibaki sent the country into political upheaval and violence that had many questioning not only the legitimacy of the election but the status of Kenya as one of the most politically stable African nations.[35] Suspicion was widespread as Odinga rejected the

---

de facto mandatory for those seeking to access most government services in the absence of other alternatives.

34. Pascaline Dupas & Jonathan Robinson, *Coping with Political Instability: Micro Evidence from Kenya's 2007 Election Crisis*, 100 AM. ECON. REV.: PAPERS & PROC. 120–124 (May 2010), http://www.aeaweb.org/articles.php?doi=10.1257/aer.100.2.120.

35. Jérôme Lafargue, ed., *The General Elections in Kenya 2007* (Mkuki na Nyota Publishers, 2004). The violence following the 2007 elections was marred by "police repression, hard-line positions by cliques, information blackout, bloody settling of scores, reactivation of ethnic tensions, political assassinations, destruction of property, deaths by the hundreds."

results and the international community expressed concern over the election's legitimacy.[36] A report published by the Human Rights Council recognized that the excess of violence was due to more than the subversion of the democratic process. The electoral injustice provided an avenue to act on long held hostility. More than 1000 individuals were killed in the post-election violence.[37] Immediate peace was due in large part to Kofi Annan, former U.N. Secretary General, who brokered a peace deal allowing Odinga to sit as the Prime Minister, a position unestablished by the Constitution, and Kibaki to remain President.[38]

The devastating effect on the legitimacy of the democratic process resulted in the establishment of a commission for review. The Kriegler Commission, as it became known, made numerous recommendations, including the creation of a new electoral management body, a legislative and political structure to accommodate such a change, and the adoption of a new voter registration system.[39] Among the voter registration recommendations, the Commission advised that a National Population Registration Database feed into a Voter Registration System. The database would include: "Personal Identification Number; Place of Birth; Gender; nationality; Marital Status; Residence; Occupation; Biometrics; Date of Death; Ethnicity/Race."[40] The call by the Kriegler commission was what many academics today fear – an Orwellian level of private information and a weaponizable tool for mass surveillance.

That is not to say the creation of such a system would not ease many administrative burdens and provide a stronger defense against fraud. If all the information were digitized, it would seemingly provide for the linking of different sub-registers to the National Population Register. Many of the recommendations may even make it easier for citizens, for example, in integrating their national IDs with their voter registration in the same database under the new regime.[41] Furthermore,

---

36. *Elections in Kenya in 2007,* DEP'T FOR INT'L DEV., https://assets.publishing.service.gov.uk/media/5a79936940f0b642860d9284/elections-ke-2007.pdf.

37. Human Rights Council, *Human Rights Situations That Require the Council's Attention, U.N. Human Rights Council*, U.N. Doc. A/HRC/7/NGO/63 (Feb. 25, 2008).

38. Mark Tran, *Kenya's Leaders Agree Power-Sharing Deal*, THE GUARDIAN, (Feb. 28, 2008). https://www.theguardian.com/world/2008/feb/28/kenya.

39. Report of the Independent Review Commission on the General Elections held in Kenya on 27 December 2007, (Sept. 17, 2008), https://kenyalaw.org/kl/fileadmin/CommissionReports/Report-of-the-Independent-Review-Commission-on-the-General-Elections-held-in-Kenya-on-27th-December-2007.pdf [hereinafter IRC].

40. This is one of the first instances in which biometrics is presented as a solution to the problems of democratic legitimacy and overall development in Kenya.

41. See IRC, *supra* note 40, at 292-93.

more immutable characteristics like fingerprinting would tackle the election fraud allegations by preventing double/multiple registration.[42] However, those developments would come at a cost to human rights, primarily in their invasive and potentially exclusionary consequences, to be discussed in further depth. One recommendation that would not threaten constitutional rights, however, was the revamping of the electoral board, verifiably lacking in institutional integrity and culpable in part for the compromised vote.[43]

B. *Rebuilding Electoral Integrity through Voter Registration*

The Kriegler Commission's revelations from the 2007 election inspired the creation of a new electoral agency known as the Independent Electoral and Boundaries Commission (IEBC), dedicated to enhancing the voter registration system.[44] The IEBC's responsibilities included the continuous registration of citizen voters and the regular revision of the voters' rolls.[45] The IEBC would be the entity later tasked with overseeing the procurement for digital identification technology and the accompanying voter registration systems as well as being harangued for its failure. However, in the aftermath of the election, the IEBC was one of the means of fighting against decades of increasingly centralized executive power, excessive corruption, and cross-regional and cross-generational inequality.[46]

1. *Digital ID's Predecessor: Voter Registration*

The lead up to the 2013 election was a harbinger of the vast digital infrastructure network that would develop over the next decade. The

---

42. *Id.* at 260.

43. *Id.* at 299. Electoral Commission of Kenya (ECK) officials had manipulated the numbers, with the Commission noting the following: "ECK Commissioners have thus announced constituency results without verifying their authenticity with the necessary statutory documentation. […] ECK shall not accept [sic] results that showed voter turnout of 100 per cent and above. The ECK Commissioners allowed returning officers who had returns over 100 per cent to "correct them." They subsequently accepted and included such results for tallying without any explanation."

44. *See Our Mandate*, INDEP. ELECTORAL AND BOUNDARIES COMM'N, https://www.iebc.or.ke/iebc/?mandate (last visited August 16, 2025) (listing the responsibilities of the IEBC in relation to election preparation and oversight).

45. *Id.*

46. *See* Mwangi S. Kimenyi, *Commentary: Kenya: A Country Redeemed after a Peaceful Election*, BROOKINGS INST. (Apr. 2, 2013), https://www.brookings.edu/articles/kenya-a-country-redeemed-after-a-peaceful-election/ (discussing the history of recent elections and the role played by the Court).

first change came about through the establishment of a biometric voter registration system with only 30 days to register 14.3 million voters.[47]

Despite the tight race, the election of 2013 was peaceful, resulting in Uhuru Kenyatta's win.[48] The turnout was 86% of registered voters, a feat that some argued represented the credibility and transparency restored through the IEBC.[49] Yet, the technology was marred by several weaknesses. Many of the fingerprint reading machines failed on the spot, allegedly due to inadequate training and logistical issues, according to the International Foundation for Electoral Systems.[50] Consequently, the legacy of the 2013 election is a mixed one. On the one hand, voter turnout hit a record high, and the aftermath of the results was notably peaceful – a significant departure from the post-election violence and allegations of misconduct in 2007. However, only two thirds of voters were successfully registered, and infrastructural weaknesses were evidenced by frequent technology glitches which resulted in the switch to manual voting, extremely long-lines, and subsequent delays.[51]

C. *The Biometric Solution Falls Short in 2013*

The new voter registration system recommended by the Kriegler Commission and implemented for the 2013 election was meant to prevent voter fraud through biometric identity verification but did not reach its potential. Namely, the IEBC failed to register enough eligible voters. In his study of the technological upgrade, Joel Barkan highlights the deception behind the IEBC's alleged registration of 79 percent of

---

47. Interview with Ahmed Issack Hassan, *IEBC Chairman Reflects on Kenya's 2013 General Elections and Future*, INT'L FOUND. FOR ELECTION SYS. (June 20, 2013), https://www.ifes.org/news/iebc-chairman-reflects-kenyas-2013-general-elections-and-future. This is not the only time the Kenyan government allotted insufficient time to rollout new technology. The same occurred during the 2017 election when the KIEMS technology was rolled out abruptly and encountered complications.

48. Jason Patinkin, *Uhuru Kenyatta wins Kenyan election by a narrow margin*, THE GUARDIAN, (Mar. 9, 2013), https://www.theguardian.com/world/2013/mar/09/kenyatta-declared-victor-in-kenyan-elections.

49. *Kenya election: Uhuru Kenyatta wins presidency*, BBC NEWS (Mar. 9, 2013), https://www.bbc.com/news/world-africa-21723488.

50. Hassan, *supra* note 48.

51. *See* David Smith, *Kenya Sees Huge Election Turnout but Violence Mostly Limited to Separatists*, THE GUARDIAN (Mar. 4, 2013), https://www.theguardian.com/world/2013/mar/04/kenya-vote-kenyatta-odinga-violence (discussing the reality on the ground for voters, such as long lines and the breakdown of voting technology); James D. Long, Karuti Kanyinga, Karen E. Ferree, and Clark Gibson, 24 J. OF DEMOCRACY 140-141, 144 (July 2013).

eligible voters, which had relied on outdated census data to support the distorted number.[52] Part of this failure can be traced to the procurement process. The Canadian Commercial Corporation provided a loan tied to the purchase of Canadian equipment through supplier Safran Morpho (presently IDEMIA), [53] which resulted in the purchase of 15,000 biometric kits. [54] However, the time required to receive bids, analyze and choose among them, and place and receive the order only left the Kenyan government four months before the election, and thirty days for registration. The investigatory piece by Barkan concluded that the procurement process, slowed by the number of bidders drawn to the lucrative contract, and ultimately split between two suppliers Safran and Face Technologies Ltd., combined too many moving pieces in too short a time, injuring the IEBC's credibility.[55] Rushing digital infrastructure projects not only sacrifices the requisite safeguards but may also compromise the functioning of the digital technology.

D. *Kenya's First Digital ID Causes a Constitutional Crisis*

Unfortunately, new complications arose in the 2017 election, which marked a second major setback in Kenya's democratization. The IEBC's failure to tally the votes correctly and another failure of the new electoral voting system led the Kenyan Supreme Court to nullify Kenyatta's victory.[56] The new program known as the Kenyan Integrated Electoral Management System (KIEMS) became synonymous with having "botched the election."[57] The KIEMS technology was composed of three parts to facilitate voting: (1) biometric voter registration; (2) biometric voter identification; and (3) electronic result

---

52. Barkan also notes the implementation of the technology was chaotic. Joel Barkan, *Kenya's 2013 Elections: Technology is Not Democracy*, 24 J. OF DEMOCRACY 156, *supra* note 45, at 164 (July 2013). Incorrect passwords were given to transmit results from polling stations and batteries stopped working, hindering the use of the technology. *Id.*

53. *The merger of Oberthur Technologies (OT) and Safran Identity and Security resulted in IDEMIA. Oberthur Technologies – Morpho becomes IDEMIA, the global leader in trusted identities*, IDEMIA (Sept. 28, 2017), https://www.IDEMIA.com/wp-content/uploads/2021/02/ot-morpho-becomes-IDEMIA-20172809.pdf

54. Barkan, *supra* note 53, at 161-162.

55. *Id.*, at 160-165.

56. THE CARTER CENTER, Kenya 2017 General and Presidential Elections: Final Report 50-1 (2018), https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/kenya-2017-final-election-report.pdf.

57. *IEBC to Upgrade KIEMS the System that Botched the 2017 Election*, NATION. https://nation.africa/kenya/news/politics/iebc-to-upgrade-kiems-the-system-that-botched-2017-elections—3363176.

transmission system.[58] According to the IEBC, the system's use of biometric registration was a "legal requirement" to "strengthen […] voter identification in the electoral process,"[59] while the use of electronic result transmission would avoid manipulation of ballot boxes.[60] However, in the event the KIEMS system failed, the return to manual voter identification by paper registration would replace biometric identification and result in two separate voting procedures, which it did.

1. *Diagnosing the KIEMS Failure – Diverging Viewpoints*

There are differing perspectives as to the root cause of the technology's failure. Some within the electoral contingent, such as the IEBC and IFES, shifted the blame elsewhere, claiming that the reliance on cellular data combined with the overload of information unexpectedly clogged the system, or what IFES President Bill Sweeney overseeing the technology called a "digital highway traffic jam."[61] Sweeney also beckoned to the "culture clash" between "vendors" who "in this space are almost always suspect," and "public servants" serving their duty.[62] In his critique of corporate interests, Sweeney alleged "there was a constant push by vendors to solve the problems so the provisional results could be posted."[63] He then went on to echo Barkan's argument relating to the 2013 election that integrating technologies from separate suppliers complicated matters.[64]

The Supreme Court of Kenya, however, conveyed a different narrative, declaring the election null and void due to "irregularities and illegalities in that election."[65] The court received testimony on the precise functioning of the KIEMS kits to investigate where the technology had encountered trouble. Testimony revealed that the kits required 3G

---

58. The Elections Law (Amendment) Act (2016) KENYA GAZETTE SUPPLEMENT NO. 157 § 2.

59. Press Statement: Verification of the Register of Voters, INDEP. ELECTORAL BOUNDARIES COMM'N NAIROBI (May 18, 2017), https://iebc.or.ke/uploads/resources/f71XGy8DwJ.pdf.

60. Cecilia Passanti & Marie-Emmanuelle Pommerolle, *The (Un)Making of Electoral Transparency Through Technology: The 2017 Kenyan Presidential Election Controversy*, 52 SOC. STUD. OF SCIENCE 928, 934 (2022).

61. Bill Sweeney, *2017 Election in Kenya: President and CEO Diary,* INT'L FOUND. FOR ELECTORAL SYS. (August 8, 2017), https://www.ifes.org/news/2017-election-kenya-president-and-ceo-diary.

62. *Id.*

63. *Id.*

64. *Id.*

65. Odinga & another v. Independent Electoral and Boundaries Commission & 2 others (2017) 42 KLR (finding irregularities in the election and ordering a new election within sixty days) [hereinafter Odinga v. IEBC et al.].

or 4G network to transmit results, and when polling stations lacked network access, officers had to move to an accessible area, and even then, the transmission sometimes failed.[66] In such a case, the move had to be made to manual transmission through the delivery of the appropriate form. The court went so far as to call the election an "ugly grouchy and reluctant mongrel of two very distinct processes" – manual and electronic. The majority overwhelmingly suggested that this was not a failing of the technology but of the administrative process leading up to the technology's implementation. At the heart of the court's ruling is the finding that the IEBC had failed to ensure access to 3G and 4G network at every polling station. The court notes this is either something the IEBC had known, or should have known."[67] In addition to the inconsistencies in the transmission of results, the IEBC failed to provide evidence in the form of access to logs and servers, to counter the hacking allegations, against the order of the court.[68] The commission had done little to demonstrate its lack of culpability when it needed to most.

French scholars Passanti and Pommerolle's ethnographic research gave credence to both the IEBC and the Court's decision, finding both the corporate and public agency at fault. Specifically, the researchers argued that any semblance of transparency was a feat of smoke and mirrors through strategic knowledge production.[69] Their critique focuses specifically on the inadequate circulation of electoral knowledge and the over-simplification of the technology as well as the problematic dynamic in which French company Safran Morpho had "seemed to have more knowledge and control over the elections than the Electoral Commission itself."[70] The concern derives from the difference in the public showcasing of "a simple and understandable technology" and the withholding of "deep information on the inner workings of technical processes," which had been requested by the opposition and again by the Supreme Court.[71]

---

66. Odinga v. IEBC et al., *supra* note 67, at ¶ 39.

67. Odinga v. IEBC et al., *supra* note 67, at ¶ 33. This goes directly against the IEBC's own contention that the "technology failed." *Id.* ¶ 86.

68. Odinga v. IEBC et al., *supra* note 67, at ¶ 38.

69. There are two forms of transparency in the electoral context, advanced by Passanti & Pommerolle, one based on communication and the other on rendering the election infrastructure invisible. Passanti & Pommerolle, *supra* note 61, at 932.

70. *Id.* at 941.

71. *Id.* at 942-43.

2. *Both the Public and Private Sector Failed KIEMS and Kenyans*

The nullification of the 2017 election and the violence that ensued were the tangible consequences of a failed attempt to increase electoral transparency. The National Super Alliance led by Raila Odinga organized a boycott against the renewed 2017 election ordered by the Supreme Court. In the second election, Kenyatta again won, this time earning 97% of the vote with more than half the electorate missing.[72] The crisis not only resulted in a significant lack of participation but renewed violence, this time against polling station staff.[73] Despite the ostensible increase in transparency in the second election of 2017, the legacy was still one of illegitimacy.

There are two narratives that emerged out of the election – one from the electoral body's side, and one from the courts – that diagnose the failure quite differently. The electoral contingency, IFES and IEBC, both point to a fundamental problem with the technology's implementation and effectuation, while the Supreme Court points to a greater infrastructural weakness rooted in poor preparation. One culprit is corporate while the other is bureaucratic. A closer look at the competing narratives beckons to the normative debate around the implementation of digital ID and the litigation strategies used to combat it.

The Supreme Court found the issue of network coverage significant in the determination of how the irregularities came about during the election, an issue rooted in the infrastructure of a developing country. The Kriegler commission recommended an updated voter registration, but the administrative process to accomplish that goal failed. Rather than rely upon a longer-term democratic process to inform the hugely influential digital infrastructure project, the IEBC tried to hastily transpose a technologically advanced system onto an inconsistently "developed" terrain.

However, it was not purely an administrative blunder, as the failure represents the failure of the private sector to effectively communicate the complexity of its technology to the public and the courts – in other words, a failure by the public and private sector. While the KIEMS kits were technologically functional, their failure to be properly understood suggests a broader partnership issue between Safran Morpho and the IEBC.

---

72. Final Report, Republic of Kenya, General Elections 2017 (January 2018), E.U. Observation Mission (Jan. 2018), https://www.eods.eu/library/eu_eom_kenya_2017_final_report.pdf.

73. *Id.* at 33.

3. *A Thought Experiment - The Tendency of Digital ID to Discriminate*

In order to understand how digital infrastructure embodies so much more than ensuring technological functions, consider the following thought experiment: The Supreme Court faulted the IEBC for being aware of this prerequisite to information transmission and failing to appropriately prepare.[74] Assuming the IEBC could not provide for universal access to 3G and 4G network, the IEBC would presumably need to move polling stations to compliant sites, resulting in discrimination to more remotely located groups. However, this type of decision could in fact disenfranchise some of the electorate. Is it the supplier's responsibility in any way to anticipate the risks its product poses to the populations it supplies? Or is it a question of political economy left to administrative bodies to resolve? These are the questions the court does not engage with yet, though they lurk beneath the surface. However, these issues would drive the litigation on the horizon against the behemoth of digital IDs – the National Integrated Identity Management System (NIIMS).

III. CONSTITUTIONAL CONCERNS: LITIGATION PATHWAY 1

NIIMS, also known as Huduma Namba, was the Kenyan government's newest attempt to improving the digital infrastructure, and in turn, the country's overall development. While NIIMS drew inspiration from KIEMS, it went far beyond electoral functions like voter registration and identification. According to Statute Law No. 18 of 2018, NIIMS functions were "to create, manage, maintain and operate a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya" using an intra-government database to assign unique national identification numbers and provide identity cards.[75] The Kenyan government intended to require registration in NIIMS "in order to access all public services."[76]

---

74. Odinga v. IEBC et al., *supra* note 67, at ¶ 33.

75. Statute Law, *supra* note 1, at 322-325, https://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMiscellaneousNo18of2018.pdf.

76. Briefing Paper, Kenya's National Integrated Identity Management System, OPEN SOCIETY JUSTICE INITIATIVE (March 2020). https://www.justiceinitiative.org/uploads/477c2588-00eb-4edd-b457-bf0d138fd197/briefing-kenya-niims-03232020.pdf

A. *Lessons from Aadhaar*

The organizations petitioning the High Court expressed concern over the sensitivity of the data collected and the linkage of such data to an undefined scope of government services.[77] The Kenyan constitution protects a right to privacy which extends to homes, property, possessions, information, and communication.[78] As part of their litigation strategy, the NGOs analogized the risks arising from NIIMS' linkage to other government services, like welfare, to those inherent in Aadhaar, the often censured Indian digital identification technology.[79] Privacy risks from both Aadhaar and the World Bank's newest identification for development initiative (ID4D) were invoked by the litigating NGOs[80] and are analyzed below for their applicable lessons.

NIIMS was in fact informed by Safran Morpho's previous digital infrastructure investment into Aadhaar, a 12-digit identity number provided to all residents of India. Both Aadhaar and NIIMS sought to create a "single source of truth," using personal demographic and biometric information to generate one's identification card. [81] The Aadhaar system is based in "stacking," so different private and governmental services can use the system to verify identity. Aadhaar identification is often used to facilitate financial transactions as well as receive access to welfare and other government services. It undoubtedly brought benefits to both the public and private sector – allowing larger swaths of the population access to capital through streamlined authentication and increasing the consumer base for banks while protecting

77. *See Nubian Rights Forum*, *supra* note 4, at ¶¶ 14-15 (summarizing the petitioning parties' claims against the government, including the intrusiveness of collecting GPS coordinates, DNA and linking the new technology to the provision of government services).

78. KENYA CONST. art. 31 (2010).

79. *See* CHRGJ, *supra* note 19, at 59 (criticizing Aadhaar for being "detached from granting any specific legal status and focused on economic or transactional identity.")

80. *See Nubian Rights Forum*, *supra* note 4, at ¶ 13 (relating Aadhaar to NIIMS, a claim advanced by petitioners).

81. *Id.* Single source of truth (SSOT) is an organizing principle in "data management and the architecture of interconnected databases that is used widely in corporate information systems which include databases managed by different entities." Tsvetelina Hristova, *The Politics of Mediation: Subjectivity, Value and Power in the Digital Grid of Aadhaar,* 16 *J. Culture & Econ.* 544, 552 (2023). About Aadhaar, DEPARTMENT OF INFORMATION TECHNOLOGY & COMMUNICATION, https://aadhaar.rajasthan.gov.in/about-aadhar.aspx. As of 2025, private actors can use Aadhaar to authenticate, a hugely contested issue during its initial release, see *Private Companies Can Use Aadhaar Infrastructure for Identity Checks Again*, https://www.lexology.com/library/detail.aspx?g=b975827d-10ba-489a-89d8-129017c01a3e.

against fraudulent activity.[82] However, as more capabilities were stacked on top of the national identification function, risks abounded.

Similar to the Kenyan technology's privacy implications, the use of mandatory biometric data was challenged on the grounds that it violated the Indian "right to be let alone," as well as constitutional guarantees against discrimination. Upon judicial review, the Indian Supreme Court allowed the program to escape largely unscathed.[83] The Court upheld the Aadhaar Act as constitutional but struck down provisions on the following: the linking of bank and SIM numbers; collection of metadata conducive to surveillance; disclosures in the interest of national security; 5-year data retention policies; and child-facing mandates.[84] Nonetheless, the decision to supply biometric data was taken away from the individual in the Indian case, which led to the immediate need for, and subsequent institution of, data privacy regulations. In addition to privacy violations, the use of a single identity card to access social benefits resulted in discrimination, both from biometric exclusion and reinforced marginalization. The lethality of that discrimination lies in its ability to deny wages and welfare benefits.[85] One of the leading academic critics of Aadhaar, Reetika Khera, claimed promoters of the ID system "packaged what was essentially a surveillance and data-mining infrastructure as a benign welfare project."[86] Khera, among others, has tied Aadhaar to "exclusion, hassles, increased hardship, and even death when people's identities could not be authenticated."[87]

---

82. *See* Yan Carrière-Swallow, Vikram Haksar, & Manasa Patnam, "A digital ID card dramatically lowers the cost of confirming people's identities." INT. MONETARY FUND (July 2021). *See also* "Open-access software standards facilitate digital payments between banks, fintech firms, and digital wallets." https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm#:~:text=The%20India%20Stack%20is%20widening,fintech%20firms%2C%20and%20digital%20wallets.

83. *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, AIR 2017 SC 4161 (India)

84. *Constitutionality of Aadhaar Act: Judgment Summary,* SUPREME COURT OBSERVER (September 26, 2018), https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/.

85. Reetika Khera, *These Digital IDs Have Cost People Their Privacy, and Their Lives*, WASHINGTON POST, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/

86. Reetika Khera, *India's Welfare State: A Halting Shift from Benevolence to Rights*, 119 CURRENT HISTORY *134, 139. (2020)* https://www.jstor.org/stable/48614527.

87. *Id.* Multiple sources have reported on deaths linked to Aadhaar's welfare benefits and discrimination. *See, e.g., Aadhaar Linked to Half the Reported Starvation Deaths Since 2015, Say Researchers*, HUFFPOST (September 25, 2018). For a discussion of

NIIMS overlapped significantly with the Aadhaar program, and therefore created the same byproduct in the absence of a proper regulatory structure – monumental risks to privacy and equity. The risk of discrimination and arbitrary denial of welfare benefits is apparent in the testimony of Ahmed Khalil Kafe, a Kenyan citizen of Nubian descent born in 1946.[88] Kafe retired from the Kenya Police Force in 1972, began a small business, and lost all his identification documents in a home theft. Mr. Kafe made an application for replacement of his national identification card in 2018 but was informed that his fingerprints were not in the records. He was asked to provide an affidavit swearing he had lost his identification documents, which he did on two occasions. Despite following up, he still has not obtained a national identity card. In 2019, he tried to register with NIIMS and was sent away.[89] The purpose of the testimony was to demonstrate the aggravating effect that NIIMS has on those seeking rightful recognition from their government and access to services they are entitled to.[90]

B. *The Nubian History of Marginalization*

The issue of access is further exacerbated by the state of identity politics and discriminatory behavior in Kenya. Ethnic division was one of the root causes of the 2007 election violence, the constitution of the Kriegler Commission, and the database recommendations that led to the creation of NIIMS. The ethnic division at issue in this case, primarily discrimination against Kenyans of Nubian descent, is a considerably different conflict from the ethnic clash between, for example, the Kikuyu and the Luo, but it still reflects a larger narrative around ethnic hierarchies and exclusion.[91] One scholar compared the ethnic division in the country to a "festering wound [which] exposed the structural rot embedded in the country's system."[92] Nonetheless, the history of

---

biometric discrimination and Aadhaar *see*, Elida K. U. Jacobsen & Ursula Rao, *Making Identity and Security through Biometric Discrimination*, *in* THE TRUTH OF THE ERROR (2018).

88. *See Nubian Rights Forum*, *supra* note 4, at ¶ 73.

89. *Id.* at ¶¶ 73-74.

90. *Id.* at ¶ 75.

91. Jason Burke, *Kenya Election: Government Accused of 'Genocide' Against Ethnic Minorities,* GUARDIAN (Oct. 27, 2017), https://www.theguardian.com/world/2017/oct/27/kenya-election-less-than-half-of-those-eligible-thought-to-have-voted

92. Shilaho Westen Kwatemba, *Ethnicity and Political Pluralism in Kenya,* 7 J. AFR. ELECTIONS, 77, 78 (2008). Nubians have been subject to additional vetting requirements, such as requiring parents to provide fingerprints or to escort their adult children when applying for identity cards and passports and even resulting in statelessness. Bronwen Manby, *Statelessness and Citizenship in the East African Community: A Study by*

ethnically imbued violence and politics cannot be separated from the discussion of Nubian discrimination at the center of the NIIMS critique. The legal ramifications and human rights risks can only be fully appreciated through study of the ethnic politics as well as the colonial legacy in Kenya – an inescapable shadow looming over this litigation.

The discriminatory practices toward the Nubian community can be traced back to the British colonial presence in Kenya. Nubians were brought from the region of Sudan in the early 20th century by British colonial forces.[93] After their forced relocation to Kenya, Nubians were denied British and Kenyan citizenship.[94] Their relationship to the colonial system has colored their experience, being "forced to go through a lengthy and humiliating vetting process in order to obtain the ID cards that are essential for everyday life," effectively being "condemned to live in poverty."[95] The African Commission on Human and People's Rights has recognized the plight of Nubians, finding violations of Articles 2, 3, 5, 12, 15, 16, 17, and 18 of the Charter, which includes: protection against ethnic discrimination and the right to equality, dignity, freedom of movement, work and pay, health, education, and family.[96]

Chairman of the Nubian Rights Forum, Mr. Shafi Ali Hussein, provided a summary of NIIMS; in particular, the linking of NIIMS and "access to identification documents, universal healthcare, fertilizer subsidies, cash transfers, affordable housing and education," and the risks posed to the Nubian community therein. Citing a report by the UN High Commission for Refugees, he confirmed that Nubians, among other minorities in Kenya, experience vetting procedures that leave them disproportionately without national identity cards.[97] Furthermore, in matters before international courts alleging discriminatory practice in identity documentation, Nubians have received judgments reaffirming the existence of such discrimination.[98] Because of the preexisting discrimination that has yet to be resolved by the Kenyan government, and the difficulty Nubians already had in identity

---

Bronwen Manby for UNHCR, UN REFUGEE AGENCY, at 32-33, (Sept. 2018). https://data.unhcr.org/fr/documents/download/66807.

93. *The Nubian Community in Kenya v. The Republic of Kenya* (Communication 317/2006) [2015] ACHPR 2, 1 (28 February 2015).

94. *Id.*

95. *Nubian Community in Kenya v. Kenya*, OPEN SOCIETY JUSTICE INITIATIVE, https://www.justiceinitiative.org/litigation/nubian-community-kenya-v-kenya

96. *African Charter on Human and Peoples' Rights*, June 27, 1981, 1520 U.N.T.S. 217; 21 I.L.M. 58 (1982).

97. *Nubian Rights Forum*, *supra* note 4, at ¶ 79.

98. *Nubian Community in Kenya v. Kenya*, OPEN SOCIETY JUSTICE INITIATIVE, https://www.justiceinitiative.org/litigation/nubian-community-kenya-v-kenya

verification and access to services, the more complicated process of registration would worsen matters.[99]

The risk NIIMS pressed upon the already marginalized Nubian community would presumably occur through the data collection process. The risk of exclusion, incorrect data, and the lack of an appeals process posed a nascent threat.[100] This is because NIIMS enrollment forms required applicants to provide a national identity card number, for which Nubians face numerous vetting processes before obtaining.[101] Therefore, Nubians would be systematically denied access to benefits through denial of the preexisting national identity cards, and as a result of the lack of government recognition, would be further excluded from the NIIMS database and its linkage to government services.

C. *Electoral Issues Resurface – A Complicit Corporation?*

Having considered the grave human rights peril to the Nubian community and the increased stakes for NIIMS, the Court took a brief look at the procurement process. The technology supplied for NIIMS was questioned due to its relationship to KIEMS and the legacy of the 2017 election.[102]

As discussed in Part II, there were different interpretations of fault relating to the delay and disorganization of the 2017 election, which led the Court to overturn the results due to inadequate electoral transparency. In the aftermath of the election, aspersions were cast on both parties, arguing the presumptive untrustworthiness of the supplier,[103] collusion between the supplier and the government,[104] and as the Kenyan court suggested, a failure on behalf of the IEBC to properly plan the procurement, rollout, and administration of the election technology.

Passanti and Pommerolle revealed a pattern of direct contracting between the government and the vendor with minimal input from the public and experts on the status of electoral technology.[105] They use the phrase 'electoral transparency through technology' to describe "a

---

99. *Id.* at ¶ 81.

100. *Nubian Rights Forum*, *supra* note 4, at ¶ 86.

101. *Id.* at ¶ 95.

102. *Id.* at ¶ 87.

103. *Id.*

104. Passanti & Pommerolle, *supra* note 61, at 932. Patrick Lang'at & Silas Apollo, *Nasa: We don't want Al Ghurair and Morpho in poll,* DAILY NATION (Sept. 18, 2017), https://nation.africa/kenya/news/politics/nasa-we-don-t-want-al-ghurair-and-morpho-in-poll—452396.

105. Passanti & Pommerolle, *supra* note 61, at 932.

socio-technical device designed by actors who construct boundaries and access through partial strategies and choices about the audience to be exposed, the procedure to be disclosed, and the technologies through which to do so, while concealing the actual debate about transparency."[106] Instead, the IEBC and vendor focused on promoting a simplified understanding of the technology as a form of pseudo-transparency. It became clear that the technology, contrary to the demonstrations provided by Safran Morpho, was much more complicated than the company publicly communicated.[107] It has yet to be fully resolved whether purposeful human interference or logistical and technological errors were the cause of the questionable election results, but the loss of public confidence in democracy was done, and Safran Morpho was associated with that loss.

The court refused to review the procurement issue on the merits due to the lack of evidence submitted by petitioners[108] but still considered IDEMIA's role in bits and pieces. While the narrative of the Court decision injured the reliability of the claims, it raised further questions about the capabilities and interests of the judicial branch. First, the Court emphasized the government's testimony that neither IDEMIA nor its predecessors were involved in the software of NIIMS, only providing the hardware carried over from KIEMS.[109] Second, the Court found that the lack of evidence precluded the judges from ruling on the procurement issue. Suspicion may arise as the contention by petitioners was that there was no public procurement process for NIIMS. However, the absence of evidence was likely because IDEMIA was not separately contracted for NIIMS; rather the Kenyan government had, according to its own testimony, repurposed the KIEMS hardware for NIIMS.[110] Nonetheless, the judges chose not to dig any further than the government testimony left open, putting the issue to bed. In a constrained judicial capacity, the Court decided not to second guess the administrative decisions of the Kenyan government, nor doubt the veracity of their claims about the procurement process. Whether the Court should have dug further given the history of corruption allegations is a worthy question, especially in light of the separate litigation against IDEMIA for the risks its technology presented.

106.*Id.* at 933.
107.*Id.* at 932.
108.*Nubian Rights Forum*, *supra* note 4, at ¶ 874.
109.*Id.* at ¶ 404.
110.*Id.*

D. *The Data Protection Act Is Not Enough*

In addition to Safran Morpho's association with past election fraud, NGO petitioners opined that the lack of data protection regulation further jeopardized the constitutional privacy rights of individuals. The 2012 Data Protection Bill, enacted after the start of the litigation, was criticized by the World Bank's own identification for development program (ID4D) analysis on Kenya.[111] The World Bank noted the gaps in the 2012 Data Protection Bill when it came to information collected under the auspices of the National Registration and Identification Bill,[112] a problem that persisted in the 2019 Data Protection Act and would be reiterated by the Kenyan Court. Because these two pieces of legislation are not linked, the Data Protection legislation has failed to include safeguards for the digital authentication, collection, storage, use, and dissemination of information as it related to the kind of personal data in the National Registration and Identification Bill.[113] The human rights implicated by the collection of this biometric information and its relationship to the NIIMS program included access to the right to education and health, related services, protection of property, freedom of movement, right to receive public services, right to presumption of innocence, freedom from self-incrimination, right to privacy and security of the person, and human dignity.[114]

E. *Resolving the Constitutional Questions*

In its determination of the case before it, the Kenyan court located three major issues – whether the legislation process leading up to enactment of the statute law was constitutional; whether the amendments violate or threaten the right to privacy; and whether the amendments violate or threaten the right to equality or freedom from discrimination. In order to evaluate the latter two questions, the court investigated the safeguards guaranteed by the Data Protection Act. The court compared the Act to "international standards," which were reduced in large part to the principles set forth by the Organization for

---

111.*Id.* at ¶ 89.

112.*ID4D Country Diagnostic: Kenya,* WORLD BANK, at 28 (2016). https://documents1.worldbank.org/curated/en/575001469771718036/pdf/Kenya-ID4D-Diagnostic-WebV42018.pdf

113.*Id.*

114.*See Nubian Rights Forum*, *supra* note 4, at ¶ 156 (noting the potential for harm given the lack of information on how the sensitive information will be collected, stored, and utilized).

Economic Cooperation and Development (OECD).[115] According to the Kenyan court, the Data Protection Act provided a set of principles to guide the "collection, processing, and transfer" of data but lacked any legislative mechanism to implement those guidelines, particularly as it applied to NIIMS.[116]

The root of the court's discontent with NIIMS was the government's lack of forethought in devising the Data Protection Act's implementation. The government provided a bare-bones rubric with no specific application to NIIMS. The court calls the missing "implementation framework" a requirement for the "adequate protection of data."[117] The Data Protection Act also failed to mention the Registration of Persons Act – the statute creating NIIMS – which left the court to infer its relationship through the former's reference to "biometric information."[118] The universality and fixed nature of biometrics, as well as the irreversible damage of data breaches required a high degree of data protection, which the Data Privacy Act did not provide.[119]

1. *Aadhaar's Legacy Returns (With a Vengeance)*

The second data privacy concern plaguing the NIIMS project is best understood in terms of its Indian precedent, and fears of "stacking" or "creeping."[120] Creeping refers to the use of data for functions outside of those originally intended. However, in the Kenyan case, creeping does not do justice to the Kenyan government's ambiguous and unspecified plan to share data across government databases.[121] The court specifically cited to the government's failure to dispute the petitioner's claim that the NIIMS database and other government databases will be linked, and in abstaining, lent credence to the petitioner's prima facie case, which predicted "invasive searches" through the unique, database-linked identifier.[122] Expert testimony regarding the risk of function creep and data breaches, both of which implicate the right to privacy, presented too great a risk for the court. According to expert Fisher, the existence of data in a centralized database creates a "temptation to use it for purposes not initially intended," removing the

115.*See Nubian Rights Forum*, *supra* note 4, at ¶ 843 (analyzing the relationship between the Data Protection Act and other instruments to regulate data).

116.*Id.* at ¶ 847.

117.*Id.* at ¶¶ 852-3.

118.*Id.* at ¶¶ 852, 885.

119.*Id.* at ¶¶ 877, 882.

120.*Id.* at ¶ 856.

121.*Id.*

122.*Id.* at ¶ 855.

informed consent obtained for the original purpose and implicating privacy rights anew.[123]

In addition to privacy, the other fundamental right that is implicated through NIIMS is non-discrimination. The Kenyan court again was swayed by the expert analysis regarding risks of exclusion from NIIMS, and the effect on access to goods and services.[124] This consisted of two broad exclusion risks: (1) those individuals who may be entitled to but unable to receive identification cards which are used for the provisions of services in both the public and private sectors; and (2) those already enrolled in biometric systems that are excluded due to authentication failure.[125]

Given the sensitivity of the biometric data, the risks of discrimination, profiling, surveillance, and identity theft, the Kenyan court found the regulatory infrastructure insufficient. Much of this reasoning arises out of a comparison with Aadhaar and the comprehensive privacy regulation enacted in India.[126] The Kenyan court frequently cites to *Justice K.S.Puttaswamy (Retd) And Anr. V.s Union Of India And Ors*, in which the Indian court recognized the potential for Aadhaar, without sufficient regulation, to wreak havoc on the right to privacy. In particular, the Indian court considered the possibility for abuse by both the government – whose ability to identify individuals with "tax records, voting eligibility, and government-provided entitlements" could create a regime of state surveillance – and the complicity of and additional abuse by the corporations that hold that data.[127]

The difficulty, recognized by the Indian Court in *Puttaswamy*, is the balance between state interest and a fundamental freedom – the right to privacy.[128] This issue occupied the Kenyan court throughout the case as well. This is why, despite the extensive discussion of risks brought on by the collection of biometric data, the court found that the collection was permissible for the specified purposes of identification. However, the request for DNA and GPS coordinates was deemed too intrusive. In the case of Aadhaar, the Indian court found this type

---

123.*Id.* at ¶ 877.

124.*Id.* at ¶ 876.

125.This includes such individuals as manual laborers, children, and the elderly. *Practitioner's Guide: Biometric Data*, WORLD BANK, https://id4d.worldbank.org/guide/biometric-data.

126.*Nubian Rights Forum*, *supra* note 4, at ¶ 855.

127.*Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*, AIR 2017 SC 4161, 175 (India).

128.*See id.* at 176 ("The balance between data regulation and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the State on one hand and individual interest in the protection of privacy on the other").

of information conducive to an authoritarian level of state surveillance. In other words, the destruction done to an individual's privacy could not be compensated by any compelling state interest.[129] The proportionality assessment was completed in both the Kenyan and Indian cases. The Kenyan proportionality test required that the law (1) have a proper purpose; (2) be carefully designed to meet the objective; (3) violate as few rights as possible; and (4) that the benefit exceed the harm to the right. The vast harm done to one's privacy by having their DNA collected and held by the government perhaps unsurprisingly is not outweighed by any benefit for identification purposes; the same is true for the tracking of individuals through GPS coordinates.[130]

Aadhaar relied on much the same analysis in locating a balance between "concerns of the state" and individual privacy. The balancing test put forth by the Indian court requires (1) a law in existence to justify the privacy encroachment; (2) a legitimate state aim, meaning one that falls within the scope of the law and is not arbitrary; and (3) that the means are proportional to the object.[131] Apart from national security interests, the interests of social welfare call for the collection of data, particularly by ensuring that "public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients." The concerns about "seeding" that Kenya invokes for its own analysis arise out of the legitimate state interest discussion. The legitimate state aim must fall within the scope of the law and be limited by the language of the statute. If the seeding of data from one database to another occurs, then the state interest is not one within the bounds of the statute, and therefore, illegitimate. The Indian court simplifies the analysis with the following imperative: the data which the state has collected has to be utilized for legitimate purposes of the state and ought not to be utilized unauthorizedly for extraneous purposes."[132] The Indian court, however, was in a less precarious position than the Kenyan court, the former able to remark broadly on the right to privacy while the latter had to confront actual data regulation. As a result, the Indian opinion, while remarkably exploratory in its philosophical discussion of privacy, may ultimately leave the question of privacy, officially a fundamental right, in such a way as to invite a robust regime for the protection of data.

The Kenyan situation was a more complex one, given that the court was faced with a presumptively invasive identification program

---

129.*Id.*

130.*Nubian Rights Forum*, *supra* note 4, at ¶ 916.

131.*Id.* at ¶ 178.

132.*Id.*

and the legislative attempt to regulate it. As a result, the Kenyan court had to consider whether sufficient protection would come out of the regulation, and whether the government was putting enough checks on its own potential abuse of the information. The collection of biometric information for the purpose of identification and authorization was weighed against the intrusion to privacy and upheld. However, the Data Privacy Act did not fare so well. While the principles of data protection were present, the requisite tools to operationalize those principles and apply them to the NIIMS project were not.[133] There is an unmistakable and dangerous gap in the approach to privacy protection by the Kenyan government: while data is encrypted and access is restricted, the lack of an operable, regulatory framework left open the possibility for the Data Commissioner to "exempt operation of the act" and "issue data sharing codes on the exchange of personal data between government departments."[134] This was the nail in the coffin, no doubt spurred on by the frightening implications of the misuse of such sensitive and powerful data discussed in the preceding pages. As a result, the Court found the "legal framework on the operations of NIIMS [was] inadequate and [posed] a risk to the security of data that will be collected in the system."[135] A risk not worth taking, seem to be the words left unsaid. Shortly after the High Court's decision on the Data Privacy Act, the death knell for NIIMS sounded.

IV. LITIGATION PATHWAY 2: CORPORATE COMPLICITY

While the previous section dove into the extensive constitutional implications of the Kenyan government's actions, the opposite side of the coin - corporate supply side litigation – occupies this section. However, before questioning whether a corporation's actions are wrongful and liability inducing, we must first inquire as to whether a corporation can, or even should, be subject to liability under these circumstances. There are different regimes of responsibility to consider which govern corporate liability; these include international regimes, through mechanisms like the Corporate Sustainability Due Diligence Directive,[136] and domestic regimes, through laws like the French Due Diligence Law.[137] Both expand the range of liability for a corporation's complicity

133.*Id.* at ¶ 853.

134.*Id.* at ¶ 1036.

135.*Id.* at ¶ 1038.

136.Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937, OFFICIAL JOURNAL OF THE EUROPEAN UNION.

137.Devoir de vigilance, *supra* note 5.

in human rights abuses. In these contemporary approaches to corporate regulation, corporate supply chains are no longer protected by the corporate form and are vulnerable to a host of claims arising out of human rights law.

The NGOs litigating the constitutional claim joined with a French organization to litigate the due diligence responsibility of IDEMIA, the firm who provided the technology for the contentious elections and whose biometric information technology was reallocated to NIIMS. IDEMIA's role in the techno-political controversy was little more than a paragraph in the Kenyan judicial decision, but before the creation of NIIMS, the company received the ire of politicians that accused it of producing untrustworthy technology. After the first election of 2017, Raila Odinga accused the soon to be IDEMIA acquired firm, Safran Morpho, of interfering in the election.[138] While the claim was never substantiated, the Kenyan court examining the election did find evidence of irregularities such as inconsistent polling practices caused by the failure of the voting kits. As discussed in Part 2 though, this was not an issue the Court attributed to IDEMIA, but to the IEBC for its haphazard planning. IDEMIA's work resurfaced in the 2021 decision in the petitioner's claims that because KIEMS was compromised, IDEMIA could not be entrusted to develop NIIMS. The petitioner's claim was not arbitrary as the 31,000 kits used for NIIMS were procured in 2018 from Safran Morpho (presently IDEMIA).[139] However, the government testimony that "no private entity, including IDEMIA, was used to develop the *software* for NIIMS" (emphasis added) led to the claim's dismissal.[140]

The Court emphasized the government's minimal reliance on IDEMIA, making the corporation's mention an oddity in this constitutional case. The Court accepted government testimony that the kits, though acquired from IDEMIA, were themselves "cleaned," meaning screened for any software, including data mining software, before NIIMS programming.[141] No software was ever acquired from IDEMIA; only the Kenyan government developed and installed all the

---

138.*French Company Rejects Opposition Claims on Vote System,* BLOOMBERG (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/french-company-rejects-kenyan-opposition-claims-on-vote-system?embedded-checkout=true.

139.Passanti & Pommerolle, *supra* note 53, at 932

140.*Nubian Rights Forum*, *supra* note 4, at ¶ 101. An investigative article by Le Monde in 2022 cast new shadows over IDEMIA's remote role in the election of 2017; while IDEMIA claimed it only provided hardware to the Kenyan government, Le Monde received reports that "the votes were indeed hosted on servers abroad, according to four sources familiar with the election process." *Inside the flaws of Kenya's electoral biometrics*, LE MONDE, May 27, 2022.

141.*Id.* at ¶ 419.

registration and encryption programs for NIIMS.[142] Therefore, IDEMIA cannot be directly liable for specific software functions or the failure thereof, but could conceivably be indirectly liable for the risks tied to the hardware it produced. The ambiguity of that accountability is where NGOs like Data Rights try to push the bounds of the law.

A. *Vigilance is not Diligence*

Data Rights, an NGO born in the aftermath of the French Intelligence Act,[143] was part of the coalition of NGOs that sued IDEMIA over an alleged violation of its Duty of Vigilance obligations under French law.[144] The legislation creates a range of corporate liability, primarily through its imposition of a due diligence obligation known as a "plan." A plan is analogous to a risk assessment, a catalogue of all the risks to human rights and the environment that a corporation poses itself and through its subsidiaries and suppliers.[145] A "plan" creates a form of civil liability that is not tied to an actual injury, but the mere potentiality of one.[146] The two remedies for this civil action are financial liability and a judicial order to amend the plan. On the one hand, this meant Data Rights could bring suit against IDEMIA for the kits in Kenya, even though the NIIMS technology was never deployed; however, it also meant that IDEMIA could not be monetarily liable without an actual harm incurred. The only other remedy provided for, an amendment to the plan, was the goal and end result of the litigation.

The claim brought by Data Rights, the Kenyan Human Rights Commission, and the Nubian Rights Forum challenged IDEMIA's due diligence plan for its failure to take into account the human rights risks created by NIIMS. The "vigilance" aspect of the plan, which requires corporations to anticipate potential human rights abuses, allowed for this form of litigation. The claim is based on the selling of IDEMIA's technology to Kenya without considering the risks of excluding already marginalized communities who struggle to register and the potential for its technology to assist government surveillance.[147] The claimants' attorneys, Slim Ben Achour and Henri Thulliez, alleged that the

142.*Id.* at ¶¶ 419, 474.

143.*Loi n. 2015-912 du 24 juillet 2015 relative au renseignement* (Intelligence Act) https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899

144.*Who We Are,* DATA RIGHTS, https://www.datarights.ngo/who-we-are.

145.Devoir de vigilance, *supra* note 5.

146.*Id.*

147.*French case against biometric tech giant IDEMIA for failure to consider human rights,* DATA RIGHTS (July 29, 2022), https://www.datarights.ngo/news/2022-07-29-kenya-due-diligence-biometric-id-case.

IDEMIA vigilance plan failed to account for any consideration of the risks.[148] While this litigation is certainly about IDEMIA's hardware, it is equally about IDEMIA's supply-side responsibility; as Lori Roussey of Data Rights puts it, companies "must pay attention to *whom* they sell their services to" (emphasis added).[149]

While the litigation in Kenya and abroad was plagued with many unknowns, there was one certainty: for one of the largest biometric giants in the world, IDEMIA's vigilance plan was, by industry standards, unsatisfactory and by human rights standards, abysmal. The entire 2021 report failed to anticipate specific consequences of its technology, instead reading like a minimally invasive risk assessment merely listing potentially relevant human rights violations.[150] Its mapping of risks found, for example, invasion of privacy and discrimination, the two issues at the center of the NIIMS case, to be the lowest of the four risk levels. Overall, the assessment was little more than a listing exercise with elusive and brief descriptions of measures, lacking any elaboration as to the specifics of its technology or its use by clients.[151]

B. *A New Plan: Rectifying Past Mistakes*

The Paris tribunal recommended mediation for the parties, which led to the settlement of the dispute and IDEMIA's updated vigilance plan.[152] A comparison of the 2021, pre-litigation vigilance plan,[153] and the 2024 post settlement vigilance plan reveals significantly more procedures for data privacy and discrimination concerns. Among the upgrades to the plan, a Group Data Protection Officer (DPO) was added to focus on countries with the lowest levels of data protection and to examine the country's political context, the end users, and local

148.*Id.*

149.*Id.*

150.*See, e.g.*, Procédure d'évaluation et actions d'atténuation des risques identifiés in *French case against biometric tech giant IDEMIA for failure to consider human rights,* DATA RIGHTS, (July 29, 2022), https://www.datarights.ngo/news/2022-07-29-kenya-due-diligence-biometric-id-case.

151.Under protective measures for human rights risks, it merely lists encryption, double authentication, data separation, management of access rights, use of pseudonyms, and anonymization. It also mentions "contractual clauses" with clients regarding data protection without further elaboration. Most human rights related information otherwise concerns labor rights. *Id.*

152.*IDEMIA Agrees to Vigilance Plan Improvements Over Kenyan Digital ID Human Rights Challenge,* DATA RIGHTS (July 29, 2022), https://www.datarights.ngo/news/2022-07-29-kenya-due-diligence-biometric-id-case.

153.*Plan de Vigilance IDEMIA 2021*, IDEMIA, https://www.IDEMIA.com/wp-content/uploads/2021/02/plan-de-vigilance-IDEMIA-2021.pdf.

legislation on personal data and cyber securities.[154] Based on the risk assessment conducted, the DPO could recommend various mitigation options, including abandonment of the project.[155] However, one of the most significant changes came under the subheading: "Risks of IDEMIA's products being misused in a context of human rights violations (e.g. discrimination, internal repression, etc.)." IDEMIA admitted that some of its products "can be diverted to uses that violate human rights" so "IDEMIA must be particularly vigilant when it comes to the use of its products."[156]

There appears little doubt that IDEMIA's updated vigilance plan was inspired by the risks inherent in NIIMS. First, the report designated which products could serve as "cyber-surveillance" technology, addressing part of the privacy concerns guiding the litigation.[157] Second, it alluded to the Kenyan case in its discussion of human rights impacts on populations. Specifically, IDEMIA brought attention to the risks the technology generates through end-user misuse, citing the example of "a civil registration system used to support discrimination against part of the population."[158] The veiled references do not stop there; the next paragraph mentions the reputational risk attached to the sale of IDEMIA technology for "electoral registration" use in countries where elections are marred by irregularities – a hint to the failed KIEMS project.[159]

C. *IDEMIA Protects (Itself) Against Exclusive Practices*

The next major change coming out of the updated plan, certainly a consequence of the pre-settlement discussions, is IDEMIA's recommendations for biometric technology in the identity domain, in which the corporation addressed head-on the risks of discrimination its product produces. It takes up several issues at stake in the constitutional litigation, shifting the legal framework guiding this controversy from that of political economy to corporate liability. First, it addresses what the NGOs before the Kenyan Court and others have termed de-duplication risks.[160] When ensuring the uniqueness of each registered

154.*IDEMIA 2024 Vigilance Plan*, IDEMIA, https://www.IDEMIA.com/wp-content/uploads/2023/03/IDEMIA-vigilance-plan-2024.pdf.

155.*Id.* at 19.

156.*Id.* at 21.

157.*Id.*

158.*Id.*

159.*Id.* at 22.

160.De-duplication refers to the process in which a biometric is entered during registration and compared against the enrollment database to ensure that the person is

individual, there is a chance of arbitrary exclusion. This "false duplicate" phenomenon is recognized by IDEMIA as having a "low probability" but that "a person should not be excluded from registration solely on the basis of the detection of a duplicate"; in the event of such possibility, IDEMIA recommends that an individual should be able to request an administrative inquiry.[161] The failure of biometrics to be recognized, particularly due to damaged fingers, is again considered to have a low occurrence rate. However, IDEMIA recommends a remediation procedure to enable access using another biometric (like iris or facial) or a pre-biometric method.[162] Finally, IDEMIA makes two recommendations that perhaps reflect a good faith effort to comply with its human rights obligations: "the implementation of these systems should not have the effect of depriving part of the population of access to public services on a discriminatory or indirect basis" and "digital identification should not be the only means of accessing basic goods and services."[163]

D. *NIIMS is Gone, but Data Rights Still Has an Agenda*

While the recommendations responded to a plethora of real risks generated by the use of its hardware in NIIMS, those same risks had already compelled the High Court of Kenya to preempt NIIMS. So then, what purpose, if any, did the French litigation serve in the aftermath of Kenya's own ruling? There are various possibilities as to the functionality of the French litigation, which was first started after the Kenyan court's own judicial findings regarding the need for greater data protection. Strategy is geared toward outcome, and the Kenyan litigation outcome had one that trumped all others - halt the roll out of NIIMS. Assuming the French litigation was not meant to beat a dead horse, the decision to litigate the largely dismantled NIIMS project in

---

not already enrolled. *A Primer on Biometrics For ID Systems*, WORLD BANK GROUP (2022), https://documents1.worldbank.org/curated/en/099025009302216641/pdf/P17159207bc5150a308b380001fc5e8e0ff.pdf. The government testimony claimed that NIIMS does not use "IDEMIA's de-duplication software" but does use its own deduplication algorithm. *Nubian Rights Forum*, *supra* note 4, at ¶¶ 419, 438. *See* CHRGJ, *supra* note 16, at 31-32 (arguing that "algorithmic de-duplication processes, which are meant to ensure that each record within a database is unique, are also often inaccurate, leading to exclusion of eligible individuals" citing Ursula Rao and Vijayanka Nair, *Aadhaar: Governing with Biometrics*, 42 S. ASIA: J. OF S. ASIAN STUD. 469, 469-81 (2019), https://doi.org/10.1080/00856401.2019.1595343).

161.*IDEMIA 2024 Vigilance Plan*, IDEMIA, at 23. https://www.IDEMIA.com/wp-content/uploads/2023/03/IDEMIA-vigilance-plan-2024.pdf.

162.*Id.*

163.*Id.*

France intimates a different set of priorities. Given that the case was started after the High Court released its decision, yet still references the dangers associated with NIIMS, it presumably hoped to prevent another attempt at NIIMS' roll out, or that of a similar program. In other words, this case, like *Nubian Rights Forum* was about the protection of marginalized communities and privacy rights in Kenya. Even though the litigation had reached the highest court, the decision was not one drenched in finality. Rather, it opened up the possibility for the Kenyan government to build a regulatory framework that would analyze the risks and provide for mechanisms to protect against privacy and discrimination risks, among others.[164] As a result, the French litigation sought change beyond this particular iteration of digital ID, likely hoping to redefine how Kenya would incorporate this new digital technology by shifting the onus to the supplier of its biometric data kits; in essence, the Data Rights contingency hoped to further insulate data privacy rights from the threat of invasive digital technology.

This litigation, however, reaches far beyond Kenya as well – to all end-users of IDEMIA products. While it may not have played an active role in protecting, for example, the Nubian community of Kenya from NIIMS, it still had precautionary implications for other vulnerable communities. In the words of one of the representative attorneys, Henri Thulliez, "without the Duty of Vigilance, this dialogue would have been unfathomable. Even if all of the NGO's demands have not been satisfied, the judicial uncertainty of mediation still brought the multinational to engage in a constructive conversation."[165] The litigation was perhaps about more than seeking justice for a particular community or country, despite the case's label *IDEMIA in Kenya*. The purpose was more progressive: to have IDEMIA confront the human rights risks it would rather list out than meaningfully tackle. The goal was to change the standard for corporations across the board.

E. *Reasons for Dual Litigation*

With aspirations to, on the one hand, prevent severe injury to the constitutional rights of marginalized communities, and on the other, reimagine how corporations relate to their risks, many of which had been deemed no more than reputational, there is a clear rationale

---

164.*Nubian Rights Forum*, *supra* note 4, at ¶ 853.

165.Henri Thulliez, LINKEDIN, https://www.linkedin.com/posts/henri-thulliez-502bb243_ngos-and-IDEMIA-agree-to-vigilance-plan-improvements-activity-7103288827636539392-P5QN?utm_source=share&utm_medium=member_desktop&rcm=ACoAACoDhFkBDcUx9J5cJB3hZz47LxL7lmztEhU.

behind the dual litigation. Even if the Duty of Vigilance can do little more than force a corporation to come to the mediation table, it gives advocates a chance to present their case and to make corporations aware of harm they traditionally turn a blind eye to.

However, that is only a surface level view. Interrogating the historical-political foundations of the context, which go beyond a mere North-South dynamic in this case, illuminates a history of corruption allegations, democratic illegitimacy, and colonial legacy. The goal may have been to make corporations accountable for how their technology is used, but an unintended consequence of these heightened standards could manifest in discriminatory sales practices. For example, one criterion used to assess the risks of a project depends on a state's designation on the democratic index.[166] More broadly, this creates a regime in which the potential developmental benefits arising out of these technologies are withheld from certain states altogether – a consequence that must be separately monitored.

Perhaps the most valuable lessons from the dual litigation strategy came out of bridging the politics and economics of the Global North and South. For example, if the litigation had only proceeded in France, the corporation's stricter compliance program could have created a barrier for developing states like Kenya to procure such services or forced the Kenyan government to blindly reform its policy in compliance with new standards. However, the constitutional arm of the litigation strategy made the Kenyan government confront its own political economy choices, while the IDEMIA arm served to reinforce the High Court's holding.

V. EPILOGUE: WHERE ARE WE NOW?

While the dual litigation strategy seemed a success, the newest iteration of digital ID in Kenya shows how the globalized effort accomplished many, but not all, of its goals. The government's newest digital ID project, Maisha Namba, has clearly been informed by the legislation that preceded it. In contrast to the mandatory biometric reliance of NIIMS, Maisha Namba is optional, government services are accessible without it, and biometrics, though used, are not stored in the database.[167] Perhaps the greatest infrastructural difference is that NIIMS was based on one master database through a new process of biometric registration, while Maisha Namba will still have a master database but

166.*IDEMIA 2024 Vigilance Plan*, IDEMIA, at 22, https://www.IDEMIA.com/wp-content/uploads/2023/03/IDEMIA-vigilance-plan-2024.pdf.

167.*Id.* at 9, 18.

will separate agency systems.[168] That being said, some organizations still believe the discriminatory risk to marginalized communities is no better than it was under NIIMS, leading to new litigation by Privacy International in Kenya.[169] As indicated at length in the previous decision, the primary source of controversy is over the data regulation meant to protect against these risks.[170] The Kenyan court issued a conservatory order in July 2024 to temporarily halt the mass roll out of Maisha Namba in response to Petitioner's affidavit that the risks under NIIMS had not been sufficiently mitigated.[171] However, the following month, the Court revoked the conservatory order, finding that doing so was not in the public interest.[172]

As the Kenyan government had stopped the rollout of NIIMS and replaced the system with Maisha shortly thereafter, there was no alternative digital ID beyond Maisha. The concern expressed by the government respondent and shared by the court was that "suspension of registration of Kenyans has very direct immediate adverse consequences on a very large population of people."[173] At the very least, though, the government has affirmed that a Data Protection Impact Assessment was performed and approved by the Data Protection Commissioner, complying with Section 31 of the Data Protection Act.[174] This is undoubtedly an improvement over NIIMS during which time there was no Data Commissioner even serving.[175] However, it is also a far cry from the international standards set forth for data privacy.[176]

168.*Frequently Asked Question*, MINISTRY OF INTERIOR AND NATIONAL ADMINISTRATION, STATE DEPARTMENT FOR IMMIGRATION AND CITIZEN SERVICES, https://usajili.go.ke/sites/default/files/2024-12/NRB%20-%20FREQUENTLY%20ASKED%20QUESTIONS.pdf.

169.*Press Statement: Civil Society seeks reform of Kenya's Digital ID System*, HAKI NA SHERIA https://drive.google.com/file/d/1gROL-gdLyJJLifgtjM39MPMEPtyT27yTE/view.

170.*Privacy International submits expert witness testimony in Haki Na Sheria's case challenging Maisha Namba, Kenya's new digital ID system,* PRIVACY INTERNATIONAL(July 5, 2024), https://privacyinternational.org/advocacy/5344/privacy-international-submits-expert-witness-testimony-haki-na-sherias-case.

171.*Haki na Sheria Initiative v Attorney General & 4 others* [2024] KEHC 10021 (KLR), ¶ 56.

172.*Id.* at ¶ 55.

173.*Id.*

174.*Id.* at 53.

175.*Nubian Rights Forum*, *supra* note 4, at ¶ 853.

176.Kiko Galpin, Jackie Jaques, Lara Ormiston, & Valerie Wilson, *A Model Governance Framework Analysis of Kenya's Maisha Namba,* INSTITUTE FOR LAW, INNOVATION, AND TECHNOLOGY, (August 2024) https://law.temple.edu/ilit/a-model-governance-

Did the government, then, surpass the court in the end by entrenching a single source of digital ID into Kenyan life that cannot be undone without severe and disruptive consequence? It appears so. Nonetheless, the dual litigation prevented a more intrusive digital ID program from becoming reality even if it could not bring the government to produce a fully transparent program with a robust regulatory structure.

VI. CONCLUSION

At the end of the day, neither litigation pathway could resolve the deep-rooted issues bubbling beneath the surface, but it could accomplish smaller, more tangible goals. The Kenyan arm of the litigation put an end to the "single source of truth" identity database whose reliance on biometric technology threatened not only to foster exclusionary data practices but to exacerbate existing tendencies toward ethnic discrimination. The Kenyan High Court may not have declared NIIMS unconstitutional, but its decision was the nail in the coffin. By belaboring the considerable risks posed by NIIMS, the Court ruled that such a technology could not be launched without a much greater investment into data protection infrastructure. In the middle of the litigation, the government had pushed through a Data Protection Act to hopefully quell concerns, but the Court was not satisfied with the rudimentary law. As a result, many were spared from the destructive consequences of potential exclusion. However, as Maisha Namba remains the only identity card, the risks of NIIMS may have only been delayed instead of dismantled.

Given the hardware had been purchased years before, the French arm of the litigation could not do much to avoid the government's decisions on questions of political economy, but it could still generate discussion and incentivize greater due diligence among corporations who supply the technology. Although it was the Kenyan population faced with risk, the NGOs involved were able to leverage the French

framework-analysis-of-kenyas-maisha-namba/. In its comparison of the regulatory framework to international principles, the Access to Justice Clinic Report finds that "GDPR requires recordkeeping of all data processing activity" and that "Kenya's Data Protection Act does not have a comparable provision but allows the Data Protection Commissioner to access records relevant to an investigation, with legal consequences for noncompliance." *Id.* Furthermore, the "Kenyan Data Protection Act exempts processing personal data that is "necessary for national security or public interest" from compliance with the Act's requirements (the "national security exception"). Because identity documents fall into this category, all processing related to the Maisha Namba is *not legally protected* under the Act the way other forms of data processing would be" (emphasis added). *Id.*

legal system to increase awareness for the exclusionary nature of such digital ID systems, particularly in developing countries where infrastructure and access vary greatly across the territory. Furthermore, by launching the two-pronged approach, the NGOs engaged in a holistic and inclusive legal approach that worked within the framework of Kenya's constitutional democracy, while still taking advantage of increased data privacy practices and human rights laws in the Global North. While a radical shift did not arise out of either litigation strategy, changes in discourse are not to be overlooked. As Duty of Vigilance claims continue to pile up in France and Kenya, and citizens organize to combat the dangers of large-scale digital identification projects, these small gains could represent big steps in the constitutional battle for our most basic human rights.