REPUBLIC OF KENYA

IN THE HIGH COURT OF KENYA AT NAIROBI

CONSTITUTIONAL & HUMAN RIGHTS DIVISION

CONSOLIDATED PETITIONS NO. 56, 58 & 59 OF 2019

IN THE MATTER OF: ARTICLES 2, 3, 10, 12,19, 20, 21, 22, 23, 24,31, 35, 93, 94, 118, 124, 165 (3) (b) (d) (ii) & (iii), 232, 258 AND 259 OF THE CONSTITUTION OF KENYA, 2010.

AND

IN THE MATTER OF: THE STATUTE LAW (MISCELLANEOUS AMENDMENT) ACT NO. 18 OF 2018.

AND

IN THE MATTER OF: THE DEFENCE, PROMOTION AND ENFORCEMENT OF THE CONSTITUTION OF KENYA, 2010.

BETWEEN

NUBIAN RIGHTS FORUM.....1ST PETITIONER
KENYA HUMAN RIGHTS COMMISSION.....2ND PETITIONER
KENYA NATIONAL HUMAN RIGHTS COMMISSION.....3RD PETITIONER

AND

THE HON. ATTORNEY GENERAL.....1ST RESPONDENT
THE CABINET SECRETARY MINISTRY OF
INTERIOR & COORDINATION OF NATIONAL GOVERNMENT.....2ND RESPONDENT
THE PRINCIPAL SECRETARY MINISTRY OF
INTERIOR & COORDINATION OF NATIONAL GOVERNMENT.....3RD RESPONDENT
DIRECTOR OF NATIONAL REGISTRATION.....4TH RESPONDENT
CABINET SECRETARY MINISTRY OF INFORMATION
& COMMUNICATION TECHNOLOGY.....5TH RESPONDENT
THE HON. SPEAKER OF NATIONAL ASSEMBLY.....6TH RESPONDENT
THE KENYA LAW REFORM COMMISSION.....7TH RESPONDENT

AND

CHILD WELFARE SOCIETY.....1ST INTERESTED PARTY
AJIBIKA WELFARE SOCIETY.....2ND INTERESTED PARTY
MUSLIMS FOR HUMAN RIGHTS INITIATIVE.....3RD INTERESTED PARTY
HAKI CENTER.....4TH INTERESTED PARTY
LAW SOCIETY OF KENYA.....5TH INTERESTED PARTY
INFORM ACTION.....6TH INTERESTED PARTY

BUNGE LA WANANCHI.....7TH INTERESTED PARTY
INTERNATIONAL POLICY GROUP.....8TH INTERESTED PARTY
TERROR VICTIMS SUPPORT INITIATIVE.....9TH INTERESTED PARTY

2ND PETITIONER'S WITNESS AFFIDAVIT

I **Alice Munyua**, a female adult of sound mind and of 2nd Harrison street, suite 175, San Francisco, CA 94105, USA do hereby make oath and state as follows: THAT

1. I am the Policy Advisor, Africa of the Mozilla Corporation duly authorized and competent to swear this affidavit.

2. I hold a Masters degree in social communications from the Pontificia Universitas Gregoriana, Rome Italy.

   Annexed herewith and marked AM-1A is a bundle of true copies of my certifications and letter of authorization from Mozilla Corporation.

3. Mozilla is the maker of the Firefox browser used by hundreds of millions of people around the world and has conducted research over several years on inter-alia the matters deponed to herein.

4. I have read and where necessary had explained to me the contents of the Petitions filed by the Kenya Human Rights Commission, the Nubian Rights Forum and Kenya National commission on Human Rights together with the Responses so far filed by the respondents named in the Petition and I understand the same. I swear this affidavit in support of the Petition by the Kenya Human Rights Commission.

5. The facts deposed to herein are derived partly from my own knowledge acquired in the course of these proceedings and partly from information obtained from the pleadings, records and documents filed in these proceedings. To the extent that any statements made herein are based on information or belief, I have disclosed hereunder the source or ground (as the case may be) of such information or belief and I verily believe the same to be true.

6. In my work with Mozilla I have gained substantial expertise and competence on issues of privacy, security, data protection and digital ID and engaged with governments around the world on the said issues.

7. In this regard, I wish to depone to the following distinct issues as relate to the amendments made to the registration of Persons Act by the Statute Law Miscellaneous Amendment Act No. 18 of 2018.

8. To begin with, there is no doubt that legal ID is generally valuable for society and legal ID schemes are enablers for the effective delivery of services and engagement between government and its citizens. The UN Sustainable Development Goals (SDGs) call for *"providing legal identity for all, including birth registration"* by 2030. Without these commonly recognized forms of official identification, individuals are at risk of exclusion.

9. At Mozilla, we recognize that Kenya appears to have various challenges with the current legal ID system. In 2015, the Office of the Ombudsman in the Commission on Administrative Justice[1] declared a crisis in the issuance of legal documentation and provided evidence of widespread discrimination in access to documentation of identity, including access to proof of citizenship. Transitioning to a digital ID system without first addressing the existing problem of widespread discrimination will not solve these problems and, in fact, will introduce several additional grave concerns including inter alia violations of privacy, security risks, increased discrimination and exclusion.

Annexed herewith and marked AM-1 is a true copy of the CAJ investigation report on the crisis of acquiring identification documents in Kenya August 2015 referred to in footnote 1.

10. Transitioning to a digital biometric ID model is not required in order to realize the benefits of legal ID. To assume that "leapfrogging" to digital ID is inherently superior ignores the risks that digital and, particularly, biometric IDs bring when deployed on a national scale.

11. The digital features and infrastructure of digital ID projects have very different implications from their analog legal ID initiatives. The addition of biometrics like iris scans, ear lobe geometry and DNA data is a dramatic expansion of the existing legal ID system and goes beyond mere digitization as the Respondents posit in their replying affidavits. Biometric and DNA linked digital ID creates profound threats of invasive privacy violations, and the potential for misuse is very high. The linking of databases has the potential to turn this system into a pervasive means of identification, tracking,

[1] http://webcache.googleusercontent.com/search?q=cache:sR9EsVg2K04J:www.ombudsman.go.ke/index.php/resource-center/investigation-reports/category/47-investigation-reports-2015%3Fdownload%3D98:stateless-in-kenya-august-2015+&cd=4&hl=en&ct=clnk&gl=us&client=firefox-b-1-d

and control, as well as increase the risk of large scale data breaches. These are serious issues that the government has to sufficiently discuss or allow the public to examine and scrutinize through public consultations.

Security, transparency, and auditability of the NIIMS project

12. It is important to see the National Integrated Identity Management System ("**NIIMS**") and other similar national biometric ID systems for what they are: a centralized database of the most intimate details of a country's residents.

13. Vide the Statute Law (Miscellaneous Amendments) Act, number 18 of 2018, authorizing NIIMS, the government contemplates collecting a wide range of incredibly sensitive information including DNA, iris scans, earlobe geometry, and fingerprints. It is not clear what purpose collecting all of this highly sensitive information serves and whether the means proposed in the law are the minimal necessary to accomplish this purpose.

14. It is a truth increasingly universally recognized that data collected is data at risk. The more sensitive information is stored in a centralized database, the more significant becomes the risk of harm to all people if that system gets breached.

15. While it is tempting to use biometrics as an easy way of ensuring the uniqueness of enrollees to a system, this use increases the risk associated with an ID system. If and when a biometric database is breached DNA and fingerprints cannot simply be reset like a password. It is also far from clear that biometrics are the only way to ensure uniqueness and avoid duplicative enrollment.

16. A breach of an ID database is not just a theoretical harm. For example, in India, despite the government's claims that the Aadhaar database was "100% secure", there have been repeated reports of the demographic data being compromised,[2] which has made it difficult to trust the resilience of the system against malicious practices. Recently, a private citizen was able to buy access to all of the demographic data in the Aadhaar database for just 500 rupees (~727 Kenyan Shillings).[3] Other reports indicate that it is possible to purchase editing rights to the Aadhaar demographic database for a mere

[2] https://timesofindia.indiatimes.com/india/210-govt-websites-made-public-aadhaar-details-uidai/articleshow/61711303.cms

[3] https://blog.mozilla.org/netpolicy/2018/01/04/mozilla-statement-breach-aadhaar-data/

2,000 rupees (~2909 Kenyan Shillings). These breaches affected more than a billion Indians and put access to several vital public and private services at risk.

Annexed herewith and marked AM 2 is a bundle of true copies of the reports referred to in footnotes 2 and 3 respectively at pages_____

17. For a second example, in Estonia, a security vulnerability called the ROCA vulnerability[4] compromised the security of more than 750,000 digital IDs issued since 2014. The Estonian system had been praised for its security and sophistication, which allowed cryptographic keys to be generated on a smartcard rather than a general purpose computer. However, when the cryptographic library was compromised, all digital IDs became vulnerable[5] and new security certificates had to be issued. Notably, despite the fact that Estonia has a small population and boasts a highly developed infrastructure and a very technologically savvy population, it was necessary to take significant measures to mitigate the risk. It is unclear whether Kenya has the resources or infrastructure to mitigate a similar breach of NIIMS.

Annexed herewith and marked AM 3 is a bundle of true copies of the reports referred to in footnotes 4 and 5 respectively at pages_____

18. As a company embracing open source[6], Mozilla has found significant benefits in open sourcing all of our code, including for products like Firefox which is used by hundreds of millions of people. This allows many individuals, including security researchers around the world, to find and report vulnerabilities in our code. With respect to the NIIMS system, the code used to generate identifiers for Kenyans should be available for public inspection, along with the code used to verify enrollment and send/share information.

19. Further, Mozilla has created a bug bounty program[7] to reward and recognize individuals who report vulnerabilities to us, which is a highly successful model that has been

[4] https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf
[5] https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/

[6] The term "open source" refers to something people can modify and share because its design is publicly accessible. The term originated in the context of software development to designate a specific approach to creating computer programs. Today, however, "open source" designates a broader set of values—what we call "the open source way." Open source projects, products, or initiatives embrace and celebrate principles of open exchange, collaborative participation, rapid prototyping, transparency, meritocracy, and community-oriented development. https://opensource.com/resources/what-open-source.

[7] https://www.mozilla.org/en-US/security/bug-bounty/

adopted by other organizations like Safaricom, Google, Microsoft, Facebook, and even the US Department of Defense. While bug bounty programs offer an important defense, we note that it is best practice for any digital ID system to undergo a professional, independent security audit at regular intervals. Reports of these audits should be made public to enhance public trust and confidence in the system.

Annexed herewith and marked AM 4 is a bundle of true copy of the details of the program referred to in footnote 7 at page_____

20. That open sourcing code can also give citizens, civil society, companies, and other stakeholders greater confidence in the system and the government's intentions. Making code and associated Application Programming Interfaces (APIs) publicly available allows anyone to audit and verify the security and privacy of the system, and would make visible many potential nefarious activities. Without this kind of transparency, it is difficult to trust a system like NIIMS.

Dangers of a centralized database like NIIMS with extensive sensitive biometric data

21. As an integrated and centralized database of sensitive biometrics, NIIMS creates a significant security risk and is susceptible to breaches by malicious actors or abuse by public authorities. The Kenyan government's statement that fears of any technical failures are "speculative and remote" ignores the multiple breaches that have plagued technology companies and governments alike; for example, the recent Marriott or Quora breach[8] and national ID systems like India's Aadhaar. This is not a remote risk. A safe operating assumption is that the database will be compromised.

Annexed herewith and marked AM 5 is a true copy of the report referred to in footnote 8 at pages_____

22. While the seamless transfer of information between government departments may be desirable for governance, there are better alternatives to achieve this without breaching privacy rights. The Government of Kenya appears to justify this choice of a centralized data system for its promise of "efficiency in the overall access and delivery of government services." However, there are examples of more secure means to this end. In Estonia, for example, the databases of each department and service provider are held

[8] https://www.wired.com/story/worst-hacks-2018-facebook-marriott-quora/

separately and are connected through the X-Road [9] data exchange layer that manages the exchange of information as needed by each program.[10] We would urge the Kenyan government to consider these alternative models that allow for communication across databases without creating a single point of failure or compromise.

Annexed herewith and marked AM 6 is a bundle of true copies of the extract of the details of the X-road referred to in footnotes 9 and 10 respectively at pages_____

23. A related concern is that the NIIMS may create a transaction log of all authentication requests linked to specific ID numbers. Access to these logs of metadata about where an individual was authenticated and by which agency could reveal highly specific information about an individual's movements and affiliations. An ID database that is primarily meant for welfare delivery should not be misused for law enforcement or intelligence surveillance. To mitigate this risk, the Kenyan government should look to decentralized models like the United Kingdom's where the identity provider does not know the purposes for which identification is requested, and the entity requesting is given minimal information restricted to confirming or denying the request.[11]

Annexed herewith and marked AM 7 is a true copy of a paper by Edgar Whitley titled 'Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach' referred to in footnote 11 at pages_____

Lack of public participation and consultation

24. The promulgation of the New Constitution in August 2010 provides a strong legal foundation for the enhancement of participatory governance through public consultation and participation in policy processes. Public participation is now a constitutional right and an obligation on the part of the government. The constitution requires that public participation be undertaken at all levels of government before government officials or bodies make official decisions that affect citizens. Direct engagement of the citizens in matters that concern and affect them is good governance

[9] https://e-estonia.com/solutions/interoperability-services/x-road/

[10] Alan Gelb, Anna Diofasi Metz - Identification Revolution: Can Digital ID Be Harnessed for Development, Center For Global Development, 2018, available at https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

[11] Edgar Whitley, Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach, https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach

practice. However, NIIMS was authorized through changes made to the Registration of Persons Act through the Statute Law (Miscellaneous Amendments) Act, number 18 of 2018, which exempted it from procedures and scrutiny that would have required introduction as a substantive bill and corresponding public debate. The amendments came into force on January 18, 2019, only 19 days after the President gave his assent without public consultation or parliamentary debate.

25. This current lack of public participation and deliberation could be interpreted as the imposition of the executive's will on the public, undermining good governance, national security, individual rights, and public trust.

26. That NIIMS has profound and serious implications for citizens as it will create a new centralized database with sensitive and unchangeable biometric data from every citizen, exposing Kenyans to various risks. The NIIMS project should therefore have been subjected to proper deliberation by the public and people's representatives in Parliament.

Insufficient and/or No legal protections for data

27. The government asserts that there is a data protection policy and bill that informed the development of NIIMS; however, this bill is still pending debate in Parliament.

28. No digital ID system should be implemented without strong privacy and data protection legislation. Data protection laws seek to protect people's data by providing individuals with rights over their data, imposing rules on the way in which companies and governments use data, and establishing regulators to enforce the laws. Individuals should always be in control of their digital identities and biometrics.

29. It is particularly egregious that NIIMS was passed even as a strong data protection law is under consideration by the Kenyan Parliament. The proposed Data Protection Bill of 2018 is a strong and thorough framework which contains provisions relating to data minimization, collection, purpose limitation, and retention limitation. If this law was in effect, NIIMS would likely be in conflict with these provisions.

30. The data protection law should establish an empowered, independent regulator to ensure rigorous regulations and standards are set on how to handle personal data processing, and public and private organizations must be compelled to be transparent and accountable, subjected to checks and balances to fulfill the rights of individuals,

and respect the rule of law. An independent data protection authority (DPA) is critical to ensure the data protection law is enforced. The authority must have the mandate and resources to conduct investigations, act on complaints, and impose fines when they discover an organization or public authority has broken the law. The data protection authority's authority and oversight should also extend to NIIMS.

31. The main features and processes of the ID system, especially those affecting the rights of users, must be enshrined in the primary law. Leaving implementation details of the NIIMS entirely to government discretion without this framework creates unacceptable risks for citizens of profiling, social exclusion, privacy violation, and security compromise. An independent regulator like a DPA can help with protecting the rights of Kenya's residents, but those rights must first be established in law.

Security has to be protected in more than just law

32. Just making an attack of a system a crime does not actually make it secure. Yet, the government has made the argument that NIIMS will be secure because section 20 of the Computer Misuse and Cyber Crimes Act, 2018 provides enhanced penalties for offences involving protected computer systems. Legal penalties alone have never served as a sufficient deterrent against malicious actors. In India, for example, despite the legal prohibitions against publishing Aadhaar numbers and breaching the system, there have been multiple public leaks and breaches, including by state governments[12]. Security must be built into the very design of the system, including basic security practices like encrypting and hashing sensitive information, using multi-factor authentication, and implementing role based access controls.

33. Another downside to relying aggressively on laws that criminalize accessing a computer system without authorization is that it can disincentivize and threaten security researchers. As noted elsewhere in this affidavit, security researchers play a critical role in finding and reporting vulnerabilities, so they can be patched in an expeditious manner. However, some of the most effective security research involves probing computer systems without the explicit permission of the owner of that system. Unfortunately, many companies and governments would prefer to bury their heads in the sand and not hear about vulnerabilities, as learning about vulnerabilities often requires dedicating resources to addressing the problem(s). However, bad actors will exploit these vulnerabilities regardless of whether we talk about them in public.

[12] https://techcrunch.com/2019/01/31/aadhaar-data-leak/ ; https://www.huffingtonpost.in/2018/07/23/how-andhra-pradesh-built-indias-first-police-state-using-aadhaar-and-a-census_a_23487838/

Ignoring the problem only makes an ID system and the deeply private information stored in it less secure.

Annexed herewith and marked AM 8 are true copies of the reports referred to in footnote 12 at pages_____

NIIMS should ensure inclusion

34. Possessing identity is increasingly a precondition to accessing basic services and entitlements from both state and private services. Given that access to vital government services will require Huduma Namba, the potential consequences of being excluded from enrolment in this system are immense. For this reason, it is important that no one is excluded from the ID system because of their physical, social, demographic, or economic characteristics. Of particular concern is the potential exclusion of marginalized communities through the process of enrolment into this system. Officials will be using existing documents to prove and verify who is a citizen, essentially locking out people who do not have these documents. This gap of conclusive proof of citizenship already affects many Kenyan communities, including the Makonde[13] the Shona along with pastoral communities and tribes.

Annexed herewith and marked AM 9 is a true copy of the report referred to in footnote 13 at pages_____

35. Those who *are* enrolled in the system might be equally at risk of exclusion due to the features of NIIMS that might end up enabling discrimination. The collection of DNA data is particularly concerning as this information can be used to identify an individual's ethnic identity. Given Kenya's history of politicization of ethnic identity,[14] collecting this data in a centralized database like NIIMS which can be linked to other databases could reproduce and exacerbate patterns of discrimination. In India too, the requirement of the Aadhaar ID number for access to HIV medication was feared to increase the risk of stigmatization and further discrimination.[15] For these vulnerable

[13] https://qz.com/africa/910868/kenyas-makonde-people-originally-from-mozambique-had-not-been-recognized-as-citizens-till-now/

[14] https://www.khrc.or.ke/publications/183-ethnicity-and-politicization-in-kenya/file.html

[15] https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar

communities, the possibility of a record being maintained and potentially being shared in unauthorized ways is an unacceptable risk.

Annexed herewith and marked AM 10 is a true copy of a report by the Kenya Human Rights Commission titled 'Politicization of Ethnic Identity in Kenya: Historical Evolution, Major Manifestations and the Enduring Implications' and the report of stigmatization of the Indian HIV population by the Aadhaar system referred to in footnotes 14 and 15 at pages_____

Lessons from other national ID systems around the world

36. The 5th Respondent's replying affidavit refers for best practice examples to several countries whose projects have been highly criticized or are not relevant comparisons. The 5th Respondent has in this regard mentioned United Kingdom, Estonia, India, and Malaysia.

37. The Estonian model, for example, which is a federated system, is in stark contrast to the integrated model put forth by the Government of Kenya. The Malaysian[16] and Indian models on the other hand have raised serious concerns for privacy, data protection, governance, and cybersecurity as well as concerns related to system design and the inclusion — or exclusion — of people from government and some private services.

Annexed herewith and marked AM 11 is a true copy of the report referred to in footnote 16 at pages_____

38. The UK DNA database referred to by the Respondents is not an ID system at all, but a forensic DNA database maintained by the UK police for those implicated in crimes.[17] It is governed by strict data retention norms which require that the records of individuals found innocent be deleted. This is in stark contrast to NIIMS which would take the DNA data of the entire population, rather than merely those suspected or convicted of crimes. In fact, the UK government's ID system, *Verify*, does not include biometrics and has a completely federated[18] ID architecture which has been commended for its

[16] David Lyon, National IDs in a Global World: Surveillance, Security, and Citizenship, available at https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1247&context=jil
[17] UK Police DNA Database, http://www.genewatch.org/sub-539478

[18] Supra note 11.

decentralized approach that gives users control.[19] The UK is also not an appropriate comparison because, like most of the other countries mentioned by the Respondents, it has had strong data protection law and enforcement in place since 1984.

Annexed herewith and marked AM 12 is a true copy of the report referred to in footnote 17 at pages 448-450

39. The Government's observation that Aadhaar, India's ID project, has been heralded as a success story ignores much of the criticism that has plagued the project. Mozilla has long argued that the Aadhaar lacks critical safeguards, and we note that the security of the system has been compromised many times. With the demographic data reportedly compromised, it is hard to see how Aadhaar can be trusted for authentication. More worryingly, hundreds of thousands of people have been denied access to basic services[20] because they either (1) do not have an "Aadhaar" (digital identity) card, or (2) their digital identity is "incomplete" because their fingerprints have not been uploaded to the national database due to poor internet connectivity.

Annexed herewith and marked AM 13 is a true copy of the report referred to in footnote 20 at pages 451-455

40. What is deposed to herein is true to the best of my knowledge, information, and belief save as to matters deponed to on information and belief, the sources and grounds whereof have been disclosed.

SWORN in NAIROBI by the said,)
ALICE MUNYUA)
)
)
This 12th day of April 2019)
)
BEFORE ME:)
)
COMMISSIONER OF OATHS)

GEORGE WANDATI
ADVOCATE &
COMMISSIONER FOR OATHS
P. O. Box 29294 - 00100
Nairobi

Deponent

[19] Supra note 11.

[20] https://thewire.in/government/aadhaar-right-to-food-pain-exclusion

DRAWN & FILED BY:
AWELE JACKSON ADVOCATES LLP
CHAKA PLACE, 2ND FLOOR
ARGWINGS KODHEK ROAD, HURLINGHAM
P.O. BOX 22701-00100
NAIROBI
Email: awele@awelejackson.co.ke
LSK/2019/00681.

TO BE SERVED UPON:

1. BASHIR, NOOR & CO. ADVOCATES
   HUGHES BUILDING 4TH FLOOR,
   MUINDI MBINGU STREET,
   KENYATTA AVENUE WING.
   PO BOX 50398-00100
   NAIROBI.

2. KENYA NATIONAL COMMISSION ON HUMAN RIGHTS
   CVS PLAZA 1ST FLOOR, KASUKU LANE,
   OFF LENANA ROAD,
   P.O. BOX: 74359-00200
   NAIROBI, KENYA

3. THE HON. THE ATTORNEY GENERAL –ATT: MR EMANUEL BITA

4. S.M. MWENDWA ADVOCATES
   PROTECTION HOUSE, 5TH FLOOR
   PARLIAMENT ROAD
   P.O. BOX 41842-00100
   NAIROBI.

5. NJOROGE REGERU & CO. ADVOCATES
   ARBOR HOUSE, ARBORETUM DRIVE
   P.O BOX 46971-00100 GPO
   NAIROBI

6. MANCO ADVOCATES
   6TH FLOOR, ACK GARDEN HOUSE,
   FIRST NGONG AVENUE.
   P.O. BOX 7619 - 00100

NAIROBI
TEL: +254(0)205160253
EMAIL: INFO@MARENDENYAUNDI.CO.KE

7. V. A. NYAMODI & CO ADVOCATES
   LOWER HILL DUPLEX, HSE NO. 7
   LOWERHILL ROAD, UPPER HILL
   P. O. BOX 51431-00200
   NAIROBI

8. RAPANDO & ODUNGA ADVOCATES.
   FORTISE SUITE, 8TH FLOOR ROOM 8.2
   HOSPITAL ROAD OF NGONG ROAD
   P. BOX 25390-00100
   NAIROBI.

9. AJIBIKA WELFARE SOCIETY
   AJIBIKA BUSINESS CENTER
   KWAME NKRUMAH STREET
   THIKA.

10. OMENKE ANDEJE & COMPANY ADVOCATES
    TOWN HOUSE, 2ND FLOOR, SUITE 6
    KAUNDA STREET
    P.O. BOX 20623-00100
    NAIROBI

11. MUTEMI SUMBI ADVOCATES
    GATE 23
    OLENGURUONE/MIJIKENDA ROAD
    LAVINGTON
    P.O. BOX 2580-00202
    NAIROBI
    MERCY@MUTEMISUMBI.COM

12. SOWETO & COMPANYADVOCATES
    BIBLICA (1ST FLOOR), OPP. KNEC
    DENNIS PRITT ROAD, CALEDONIA
    P.O BOX 44287-00100
    NAIROBI

13. BUNGE LA WANANCHI

14. MBUGUA, ATUDO & MACHARIA ADVOCATES
    2ND FLOOR, JADALA PLACE NGONG LANE,
    OFF NGONG ROAD
    P.O. BOX 10409-00100
    NAIROBI