

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
CONSTITUTIONAL & JUDICIAL REVIEW DIVISION
CONSOLIDATED PETITIONS NO. 56, 58 & 59 OF 2019

BETWEEN

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

VERSUS

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

AND

CHILD WELFARE SOCIETY.....1ST INTERESTED PARTY
AJIBIKA SOCIETY.....2ND INTERESTED PARTY
MUSLIMS FOR HUMAN RIGHTS INITIATIVE.....3RD INTERESTED PARTY
HAKI CENTRE.....4TH INTERESTED PARTY
LAW SOCIETY OF KENYA.....5TH INTERESTED PARTY
INFORM ACTION.....6TH INTERESTED PARTY
BUNGE LA WANAINCHI.....7TH INTERESTED PARTY
INTERNATIONAL POLICY GROUP.....8TH INTERESTED PARTY

TERROR VICTIMS SUPPORT INITIATIVE.....9TH INTERESTED PARTY

JUDGMENT

INTRODUCTION

1. On 20th November 2018, the National Assembly enacted Statute Law (Miscellaneous Amendment) Act No. 18 of 2018. The President of the Republic of Kenya gave his assent to the said Act on 31st December 2018, and it commenced operation on 18th January 2019.

2. The effect of the Act was to amend several provisions of a number of existing statutes, among them the Registration of Persons Act (Cap 107 of the Laws of Kenya) (hereinafter referred to as “the Act”). The amendments to the Act establishes a National Integrated Identity Management System (hereinafter “NIIMS”) that is intended to be a single source of personal information of all Kenyans as well as foreigners resident in Kenya.

3. A new section 9A was introduced to the Act by the amendments, and it established NIIMS in the following manner:

“9A (1) There is established a National Integrated Identity Management System.

(2) The functions of the system are —

(a) 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;

(b) to assign a unique national identification number to every person registered in the register;

(c) to harmonise, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons;

(d) to support the printing and distribution for collection all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification cards issued under the Births and Deaths Registration Act, Basic Education Act, Registration of Persons Act, Refugees Act, Traffic Act and the Kenya Citizenship and Immigration Act and all other forms of government issued identification documentation as may be specified by gazette notice by the Cabinet Secretary;

(e) to prescribe, in consultation with the various relevant issuing authorities, a format of identification document to capture the various forms of information contained in the identification documents in paragraph (d) for purposes of issuance of a single document where applicable;

(f) to verify and authenticate information relating to the registration and identification of persons;

(g) to collate information obtained under this Act and reproduce it as may be required, from time to time;

(h) to ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register;

(i) to correct errors in registration details, if so required by a person or on its own initiative to ensure that the information is accurate, complete, up to date and not misleading; and

(j) to perform such other duties which are necessary or expedient for the discharge of functions under this Act.

(3) The Principal Secretary shall be responsible for the administration, coordination and management of the system.”

4. Section 3 of the Act on interpretation was also amended to include the following new definitions:

*“Insert the following new definitions in proper alphabetical sequence-
"Biometric" means unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form;*

"Global Positioning System coordinates" means the unique identifier of precise geographic location on the earth, expressed in alphanumeric character being a combination of latitude and longitude; "physical form" means existing in a form that one can see and touch; and "Principal Secretary" means the Principal Secretary in the ministry responsible for matters relating to registration of persons.”

5. The Nubian Rights Forum (the 1st Petitioner), the Kenya Human Rights Commission (the 2nd Petitioner), and the Kenya National Commission on Human Rights (the 3rd Petitioner), are aggrieved with the amendments made to the Act, which they claim were passed in violation of the Constitution and in bad faith and pose serious and immediate threats to fundamental rights and freedoms protected under the Bill of Rights. They therefore respectively filed Petitions in this Court, namely Nairobi High Court Petition No 56 of 2019, Nairobi High Court Petition No 58 of 2019 and Nairobi High Court Petition No 59 of 2019, which petitions were subsequently consolidated for hearing by this Bench.

6. The position taken by the Petitioners was supported by Muslims for Human Rights, Haki Centre, Law Society of Kenya and Inform Action which were joined to the proceedings as the 3rd, 4th, 5th and 6th Interested Parties respectively.

7. The Respondents in the Consolidated Petitions are the Honourable Attorney General (the 1st Respondent); the Cabinet Secretary, Ministry of Interior and Co-ordination of National Government (the 2nd Respondent); the Permanent Secretary, Ministry of Interior and Co-ordination of National Government (the 3rd Respondent); the Director of National Registration (the 4th Respondent); the Cabinet Secretary for Information, Communication and Technology (the 5th Respondent); the Speaker of the National Assembly (the 6th Respondent); and the Kenya Law Reform Commission (the 7th Respondent).

8. The Child Welfare Society of Kenya, Ajibika Society, Bunge La Mwananchi, International Policy Group and Terror Victims Support Initiative being the 1st, 2nd, 7th, 8th and 9th Interested Parties joined the Respondents in opposing the Petitions.

9. The Petitions proceeded to hearing by way of affidavit evidence, oral testimony including by expert witnesses, and written submissions which were highlighted by the parties. We need at this stage to draw attention to the fact that after completion of the hearing, and before delivery of judgment, the Data Protection Act No. 29 of 2019 was enacted by the National Assembly. The 6th Respondent thereupon sought directions from the Court in light of this development. The Court considered it prudent that the parties be given an opportunity to comment on the Data Protection Act and set a further hearing date to receive submissions in this regard. We set out hereunder the respective pleadings and evidence by the parties. For convenience, we shall summarise the cases for the principal parties alongside the respective cases of the Interested Parties who supported their positions.

THE PETITIONERS' CASES

The 1st Petitioner's Case

10. The 1st Petitioner, the Nubian Rights Forum, is a human rights organization that advocates for the rights of the Nubian community in Kenya. Its Petition is dated 14th February 2019 and is supported by the affidavit of its Chairman, Mr. Shafi Ali Hussein, sworn on even date and a further affidavit sworn by the said deponent on 12th April 2019. Additional affidavits filed by the 1st Petitioner were sworn on 11th April 2019 by Dr. Thomas Fisher, a Research Officer with Privacy International, and on 12th April 2019 by Ms. Fatuma Abdulrahman and Mr. Ahmed Khalil Kafe, both members of the Nubian community.

11. The 1st Petitioner also filed a witness statement by Mr. Anand Venkatanarayanan, who gave oral testimony as one of the expert witnesses for the Petitioners. Mr. Shafi Ali Hussein, Ms. Fatuma Abdulrahman and Mr. Ahmed Khalil Kafe were also cross-examined on their affidavits at the request of the 4th and 7th Respondents.

12. The 1st Petitioner is aggrieved by several aspects of the impugned legislation, including its implementation. The first aspect of its case is that in order to constitute the NIIMS database established under section 9A of the Act, the government commanded that Kenyan citizens and foreign nationals provide sensitive personal information purportedly to establish, verify and authenticate their identity, and subsequently receive a unique identity number, known as *Huduma Namba*, through a 30-day nationwide mass biometric registration exercise.

13. The 1st Petitioner contended that the technical specifications and planned practical implementation of NIIMS was opaque, with inadequate and conflicting information provided to the public. Its position was that the process by which the NIIMS system has been established and the information revealed to date concerning its design, implementation and administration strongly suggests that the lessons from international experiences with digital identity systems have not been sufficiently reviewed and applied by the Respondents. The experiences and challenges of the Aadhaar system in India were cited as an illustration of the problems likely to be encountered with NIIMS.

14. The 1st Petitioner further contended that even though the government has stated that it would not collect Deoxyribonucleic Acid (DNA) and Global Positioning System (GPS) coordinates, the legislative amendments place no limits on the scope of data that can be captured and stored in the NIIMS database.

15. The second aspect of the 1st Petitioner's grievance against NIIMS, as we understand it, is with regard to its linkage to the delivery of an undefined sphere of government services, including access to identification documents, universal healthcare, fertilizer subsidies, cash

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 4 of 205.

transfers, affordable housing and education. The 1st Petitioner complained that members of the Nubian community have challenges acquiring identity documents under the existing system under section 8 of the Act. It claimed that the section grants registration officers broad authority to demand additional evidence from persons from marginalized areas, and entails an onerous process of establishing their Kenyan nationality in order to receive a national identity card.

16. It was its argument further, that the discriminatory practices against the Kenyan Nubian community has been recognized at the regional level by the African Commission on Human and People's Rights in the **Nubian Community in Kenya vs Republic of Kenya (Decision of February, 2015)**, and by the African Committee of Experts on the Rights and Welfare of the Child in **Children of Nubian Descent in Kenya vs Kenya (Decision of March, 2011)**. Furthermore, that both tribunals found that Kenya's discriminatory registration and identity documentation practices infringe on the rights of members of this minority.

17. The gravamen of the 1st Petitioner's case therefore, is that NIIMS will aggravate the discriminatory practices against the Nubian community, as it will be linked to the provision of essential government services. According to the 1st Petitioner, their access to identity documents is already unequal, and the mass biometric registration requiring submission of state-issued documentation, threatens to further exclude and disenfranchise persons from marginalized areas.

18. The 1st Petitioner's third challenge to NIIMS related to the process of procurement, design and establishment of NIIMS. It contended that IDEMIA (previously or concurrently operating as Morpho/OT-Morpho/Safran Identity and Security) which has been tasked with the process of data collection under NIIMS, has been implicated regarding lack of proper delivery of services both in Kenya and other countries such as Ghana. It was its contention that there is no public record of the procurement process for the design of NIIMS, and that the tender could have been awarded before the impugned law was enacted.

19. The fourth challenge raised by the 1st Petitioner is on the process of enactment of the Statute Law (Miscellaneous Amendments) Act No. 18 of 2018. It was averred that the Bill was never presented to, debated or passed by the Senate, yet according to the 1st Petitioner, this is the constitutional way through which members of the public participate in the passing and amendment of laws.

20. The 1st Petitioner further contended in this regard that counties have a direct interest in the registration of persons, as part of their functions relate to county planning and development including the use of statistics. It contended therefore, that failure to submit the Statute Law (Miscellaneous Amendments) Bill to the Senate for consideration was a violation of Article 96 of the Constitution.

21. It was also the 1st Petitioner's case that the use of a miscellaneous amendment procedure for the establishment of NIIMS denied the concerned communities adequate opportunity to know about the issues and participate in its establishment as required under the Constitution. Further, that the Miscellaneous Amendment Bill was an "omnibus Bill" which obfuscated and combined many issues, making it extremely difficult for citizens to engage effectively with the process. According to the 1st Petitioner, it is only proper to use the procedure of Statute Law Miscellaneous Amendments in cases of minor, non-controversial corrections of legislation.

22. The 1st Petitioner further challenged the process of enactment of the impugned amendments on the basis that the right to public participation was not observed. It contended that the concerned communities were not accorded a reasonable opportunity to know about the issues or have an adequate say in the amendments. It further argued that since the enactments, the government has not sensitized its citizens on the far-reaching effects of data collection.

23. The fifth and last concern raised by the 1st Petitioner was that there is no law in force to guarantee the privacy provisions in the Constitution, given the invasive process proposed to be implemented through NIIMS. It was its case that it is the right of every person to have their right to privacy, which includes homes, property, possessions, information and communication, protected. The 1st Petitioner raised particular concern with the requirement for Global Positioning Systems Coordinates (GPS) and Deoxyribonucleic Acid (DNA), among other biometrics. It asserted that GPS targets an individual's communications and their exact whereabouts, which is very intrusive into one's right to privacy, while the definition of "biometric" in the Act permits the collection, storage, and retention of an inordinate amount of data.

24. The 1st Petitioner contended, in addition, that there are insufficient safeguards in the existing laws to protect the personal data that will be collected. Further, that there are no effective measures to ensure that the data will not be accessed by persons who are not authorized by law to receive, process and use it, or that it is not used for purposes incompatible with the reason for its collection. It was also its contention that the amendments to the Act are silent on whether citizens will be able to have access to the information gathered, and whether they can ask for incorrect data to be deleted or rectified.

25. Lastly, it was the 1st Petitioner's case that the impugned amendments do not comply with core data protection principles on consent and legitimacy, fair and lawful processing, purpose and relevance of data, management of the data lifecycle, transparency of processing, as well as confidentiality and security of personal data. It contended that the Data Protection Bill 2018 that was then going through the legislative process was "*confusing, mixes concepts, lacks clear objectives and key definitions and otherwise leaves many loopholes.*"

26. The 1st Petitioner therefore asked the court to grant the following orders:

a) A declaration that section 3, 5 & 9 of the Registration of Persons act as amended by the Statute Law Miscellaneous (Amendment) Act 2018 are unconstitutional for infringing the right to privacy, dignity, socio-economic rights, the right to public participation and the right to equality and non-discrimination.

b) A declaration that Sections 3, 5 & 9 of the Registration of Persons Act as amended by the Statute Law Miscellaneous (Amendment) Act 2018 are unconstitutional because the manner in which they were amended and the procedure thereto was constitutionally infirm.

c) A declaration that implementation of Sections 3, 5 & 9 of the Registration of Persons Act as amended by the Statute Law Miscellaneous (Amendment) Act 2018 is unconstitutional because the State has failed to provide statutory framework to protect the right to privacy and protection of data.

d) A declaration that the State must implement the decisions of the African Commission on Human and Peoples' Rights and the African Committee on the Rights and Welfare of the Child in the cases of, respectively, Nubian Community v. Kenya and Children of Nubian Descent v. Kenya before commencing on NIIMS registration process.

e) An order declaring that Section 3, 5 & 9 of the Registration of Persons Act as amended by the Statute Law Miscellaneous (Amendment) Act 2018 are unconstitutional.

f) Costs of this suit be provided for.

The 1st Petitioner's Evidence

27. In his witness statement, Anand Venkatanarayanan, who testified as PW2, described himself as an expert on Cyber Security and Computer Fraud Forensic Analysis, with a special interest on Financial Modelling. He stated that he graduated in 1998 with a Bachelor's degree, with distinction, in Technology with a Computer Science Major from the University of Madras. He stated further that he has 21 years' experience in various aspects of computer software, and had given affidavit evidence as a cyber-security expert in the Aadhaar case in the Supreme Court of India in support of the petitioners therein.

28. Mr. Anand stated that upon review of the Petition by the 1st Petitioner, the 1st and 2nd Respondents' replying affidavits, and the relevant accompanying documentation, he had made several conclusions on NIIMS. The first was that NIIMS is functionally and architecturally similar to the Indian Aadhaar system. His second conclusion, based on the first, was that it would result in the same outcome, namely an endeavour which would pose a massive risk to personal security and privacy of the Kenyan residents with no demonstrable benefits. Lastly, that it would also create national security risks to Kenya, which would be impossible to mitigate.

29. Mr. Anand stated that a foundational assumption underlying the logic of the NIIMS system is that the use of biometrics assures that there is no duplication in the registration of individuals. Further, that the assumption behind biometric identifiers is that there exists a part of the human body that is unique to an individual, and we can use a digital representation of that part to uniquely identify the individual from across the entire population. It was his evidence, however, that biometrics are fallible and cannot be relied upon as unique identifiers for the purposes of deduplication. His averments, as we understand them, are that firstly, to claim that a particular biometric parameter is unique across all time is mathematically infeasible. This is for the reason that one would need to have data for past and future populations to be able to reach this conclusion, which is not possible for future populations.

30. Mr. Anand stressed, secondly, that biometrics are affected by ageing and time, and that every single cell and part of the human body ages and changes, and events in life such as disease or constant manual work can accelerate it. It was his averment therefore that the assumption of uniqueness with respect to biometrics is true only within a time range. He nevertheless noted that biometrics are stable after the age of 15 years, but *"wildly variable before that."*

31. It was his averment, thirdly, that the identification of a person by a human being is a different process from that of identification by a machine or algorithm, and that human beings can identify others accurately because of the *'evolutionary pressure to reproduce.'* It was his

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 7 of 205.

view therefore, that while a human being cannot fail to identify the gender of another human being, an algorithm uses different means to identify people through computation and has to use different conceptual constructs.

32. Mr. Anand explained in technical detail the concepts that are used in algorithms, including the use of points in fingerprints matching, to illustrate that a perfect overlap of points and matching of fingerprints is impossible because of extraneous factors such as sweat, tears, physical position and other mechanical factors. It was his averment therefore that thresholds are specified to identify a person through such matching of points. Mr. Anand's contention was that there is an inherent conflict with the said thresholds for the reason that if a very high threshold is set, such as 99% matching of the points, it will enable a person to enroll twice at different points of his life, because ageing changes biometrics. On the other hand, that if the threshold is low, then some enrolments will be identified as duplicates and genuine persons would not be registered.

33. Mr. Anand's testimony was that this is a problem that arises from the nature of biometrics and cannot be worked around or fixed. Our understanding of his argument, which was made in relation to the Aadhaar system in India, is that a person who had not previously enrolled or registered in the system could be identified as having been registered and rejected. Conversely, a person who was already enrolled could, after some lapse of time, be identified as not having been enrolled, and allowed to register a second time because of ageing biometrics. His assertions on this point were based on an article he had published on the internet on the Aadhaar project, the relevant website address of which was given, which made reference to a paper published in the Economic and Political Weekly by the Centre for Internet and Society (CIS). It was his contention, on the basis of this paper, that enrolment rejection rates will accelerate as the size of the database increases.

34. Mr. Anand gave an example of the errors of duplication noted in the Aadhaar system which is operated by the Unique Identification Authority of India (UIDAI). He observed that UIDAI used OT Morpho's algorithms, the same algorithms which, to his knowledge, are also being used in the NIIMS in Kenya. He placed reliance on an online article by Dr. Hans Varghese Mathews titled "**Flaws in the UIDAI Process**" published in the Economic and Political Weekly, 26 February 2016, LI No. 9 which found that in India's population of approximately 1.2 billion, approximately 10 million people (0.8%) would be excluded from the system as a result of false positive matches.

35. According to Mr. Anand, independent research conducted over a period of time had established that deduplication is by no means a natural consequence of the introduction of an identification system that relies on biometrics. His opinion was that the Kenya government had not taken this body of evidence into account, given its over-reliance on the assumption that biometric uniqueness is beyond question. He further expressed the view that because the reliability of any biometric-based identification system depends on mathematical calculations, it is critical to have public disclosure of the technical data on the deduplication algorithm, and that this should be published along with the sample data so that experts can analyse it. His testimony was that he was not aware that the Kenyan State had publicly disclosed the algorithms used to identify "duplicate" biometric data.

36. It was Mr. Anand's evidence that there could also be failure of biometrics at authentication stage. He defined 'biometric authentication' as a comparison between the biometric parameter (iris or fingerprint) *versus* what was stored during enrolment and termed

it as a biometric comparison across time. He took the position that for this to succeed all the time, an important pre-condition must exist, namely the condition of immortality or, in other words, that the individual's chosen biometric parameter does not change across their entire life time. This, he stated, is not the case for both iris and fingerprints, and even for DNA, as mutation or a radiation exposure alters DNA.

37. Mr. Anand testified that while laboratory results on biometric authentication show a high probability of success of around 99%, the real-world data is very different. It was his testimony that women and poorer citizens, including manual labourers, domestic workers, homeless people, and agricultural workers were the most likely segments of the population to be excluded by biometric authentication. He supported his averment by citing the experience in India, where studies demonstrated high rates of exclusion. He further cited section 5 of India's Aadhaar Act which, although not yet adequately implemented to date, at least recognizes that special measures would be needed to address exclusion of large categories within the population. He concluded that to his knowledge, Kenya has no such provision in connection with the implementing legislation authorizing the establishment of NIIMS.

38. On the security of data collected through NIIMS, Mr. Anand averred that it is self-evident in computer security that nothing is truly secure, and the relevant considerations are the costs and benefits of collecting and keeping data. His view was that centralised databases such as Aadhaar and NIIMS hold so much data that the cost- benefit ratio tilts in favour of hackers or those who want to compromise the personal data. It was his testimony that the number of times the Aadhaar database has leaked is beyond counting. Further, that data leaks caused by centralization is not a perception, but an outcome that can neither be avoided nor mitigated. According to Mr. Anand, this realization forms the basis of the design of modern-day computer systems where decentralization becomes the central design principle. He termed NIIMS as an archaic design compared to modern-day system architectures and equated it to *"a horse-bungee drawn by a lame horse on the digital highway"* whose digital journey was bound to end in failure.

39. With regard to how NIIMS would negatively affect Kenya's security, Mr. Anand averred that given the complexity of the NIIMS project, all parts must be audited through public disclosures or else terrorists or spies can infiltrate the NIIMS system by exploiting its inherent weakness. It was his averment that this happened in Aadhaar, where numerous cases of enemies of the state masquerading as citizens obtained Aadhaar numbers. He made reference to various internet sources for this statement, and concluded that it is in the public interest that the state discloses the algorithms and systems used to construct the NIIMS project for national security reasons.

40. Mr. Anand's conclusion was that the NIIMS project is functionally, architecturally and technologically similar to the Aadhaar system and suffers from the same flaws. In his view, while the Kenyan government may promise that it will not repeat the same mistakes, it does not have the technological capability to honour the promise, as is evident from its claim that NIIMS is different from Aadhaar. Further, that while the harmonization of the various databases that contain personal data is a laudable goal, the Kenyan government has not done a detailed cost- benefit analysis of such an approach and other alternatives. Mr. Anand referred to and cited studies done in India on the Aadhaar project which indicated that the costs were high compared to the benefits it offered. His parting shot was that the NIIMS project would thus be a waste of public money, which money could have effectively been used elsewhere.

41. When cross-examined by Dr. Nyaundi for the 5th Respondent, Mr. Anand stated that he was self-taught on computer security. Further, that he has taught cyber security classes to the police. He, however, conceded that he had not attended any class to receive training on cyber security. His testimony was that he had written articles which he posted on the internet but had not been published in any peer-reviewed academic journals. However, that one of his articles was edited and discussed by people interested in the subject of cyber security.

42. Mr. Anand conceded that he had written the said articles prior to the implementation of NIIMS. He also accepted that he had not worked on NIIMS, reviewed any documents on it, or interacted with the system. He, however, stated that he studied the objectives of NIIMS, the architecture of the system, and the need for a single identifying number based on biometrics. It was his evidence that he could not tell whether Kenya had used the OT Morpho algorithms, but had reached the conclusion that it had because the OT Morpho algorithms are the ones normally used for biometric deduplication. He also confirmed that he did not know the software Kenya used in NIIMS.

43. Mr. Anand agreed that one of the problems with the Aadhaar system was that the data was inaccurate because the data collectors were paid by the number of persons enrolled, hence leading to the temptation to exaggerate the numbers. He nevertheless maintained that the Kenyan system was similar to the Aadhaar system. He conceded that he was not part of the team that designed the Aadhaar system but asserted that he had investigated its design and architecture from available public material.

44. Mr. Anand explained that a centralised system means that all the data is kept in a single database. His evidence was that most countries divide the data into smaller functional databases and only retain the personal core data in a central database. Further, that the functional databases are referred to as federated databases, and are not decentralized databases, as they do not have any link to the central database. It was his position that NIIMS is both centralised and federated, which is what informed his criticism of the system, as the federated databases still have back references to the central database. His view was that the NIIMS system is a single central national data base having all records of the individual.

45. According to Mr. Anand, biometric identification is in itself not bad technology, as it can improve security, and a single identity system is a global trend. Further, that electronic data was under constant threat globally. Additionally, electronic storage is gaining global currency as that was where the world was going, and he was not advising any country to go back to the age of paper.

46. His evidence was that every electronic storage system must have protection, but that the protections provided by governments are usually not sufficient. According to Mr. Anand, electronic data is usually protected by layers of access. That some people have full access, some less access and others minimal access. He was not aware of the Kenyan laws on protection of data, and without public information, he could not specifically say what the weaknesses of NIIMS were. He nonetheless asserted that his complaint about NIIMS was not about digitisation but its architecture, which has no limitations on the purposes of the system, and which allows breaches, frauds and exclusion.

47. In response to questions from Mr. Njoroge Regeru for the 2nd and 3rd Respondents, Mr. Anand told the court that the Open Society Foundation had sourced him as a witness in the petition. His brief was to make the court understand the various aspects of the NIIMS project,

and he reiterated that he understands the architecture of NIIMS from its technical purposes which have been disclosed to the public.

48. It was his evidence that while he had filed an affidavit in the Supreme Court of India to oppose Aadhaar, the Court had restricted the use of Aadhaar but did not outlaw it. He had not testified before the Supreme Court. He disagreed with the proposition that he is not an expert of international standing on cyber security, insisting that he gives industry- wide technical talks on the subject, and is a key panelist in an international cyber security conference held annually in India. He stressed that based on the pleadings filed in this Petition, he had formed the opinion that NIIMS and Aadhaar are functionally and architecturally similar. He conceded that he had not read any technical document on NIIMS.

49. He disputed various statements made in the pleadings filed by the Respondent's experts, and his evidence was that deduplication is not based on biometrics alone, and that minimal personal information is required for identification. His opinion was that NIIMS did not observe data minimization and purpose limitation standards. He admitted that most countries develop their data capture programmes and encryption algorithms locally, and stated that he had not seen any such software that was locally developed for NIIMS, nor talked to any of the local experts who designed the system.

50. Mr. Anand stated that although he did not doubt the technological competence of Kenyans, there should be information made available on the NIIMS to build confidence in the system. He stated that identity projects create mistrust for lack of information. Mr. Anand also testified that he was familiar with the distinction between open source and closed source software but disputed that data in closed source software will guarantee the safety of personal data. His opinion was that open source software invites continues scrutiny and improvement, and gave an example of the public disclosure of the Aadhaar system in India. In his opinion, the technology design for NIIMS should be publicly disclosed.

51. Mr. Anand disputed the demonstrable benefits of NIIMS, stating that they are not based on any data. He was emphatic that given its current architecture, NIIMS will not achieve its stated objectives, and that its costs outweigh its benefits. He admitted that he had discussed the disadvantages of NIIMS but not its benefits, stating that people tend to overestimate the advantages and fail to talk about the disadvantages. Further, that the statement that NIIMS is a single source of truth is a conflation between identification and identity, and the database is used for identification not identity purposes. He was also doubtful whether such a biometric system can isolate terror risks or enhance security, asserting, by way of illustration of his position, that there were 45 – 50 reported cases of attempted infiltration of the Aadhaar system in India.

52. Mr. Anand denied that his conclusions on the weaknesses of biometric systems are limited to those that use fingerprints alone, noting that the Aadhaar system used other biometric and demographic markers. In his view, irrespective of whether a system is a single modal or multimodal, it is still exposed to the risk of deduplication. He explained that a multi-modal system uses various demographic and biometric parameters as opposed to only one parameter that is used in a single-modal system. He testified that it was reasonable to state that NIIMS is a multi-modal system, but did not accept that it had factored in deduplication. He reiterated that he was skeptical about the use of fingerprints and that data from India had shown the ageing of fingerprints of persons who undertake manual work.

53. While agreeing that biometric identifiers cannot be discounted, Mr. Anand pointed out that there is a threshold required to be met to ensure probability of success, which has not been publicly disclosed about NIIMS. He also noted that the fundamental problem of using biometrics is the impact of failure, and although no system is perfect, there is need for the right architectural design of the system and mitigation measures.

54. When cross-examined about his statement on the likely exclusion of women and the poor by the system, Mr. Anand stated the statement was made in reference to South Asian countries. He nevertheless insisted that unless he sees data-based evidence, he would still hold the same opinion about NIIMS.

55. Mr. Anand agreed that terrorism is a threat worldwide. His evidence was that terrorists will try to hack and gain access to systems. However, the threats would be minimised where correct expertise is applied. He denied suggestions put to him by Mr. Regeru that he was not an expert; that he was a partial witness; that he did not have any experience or knowledge of NIIMS; that his conclusions were based on conjecture and speculation; and that he was dismissive of local content and expertise.

56. In cross-examination by Mr. Bitta, the Counsel for the 1st Petitioner, Mr. Anand conceded that digitisation brings better service delivery and that countries cannot go back to the paper age. In his view, however, the law cannot fix what technology has broken, so that if there are mistakes in the system design, the law may not assist. He also stated that a functional data protection law will only exist where the system has the right architecture. He denied that he was a hacker, stating that he is a security researcher, and that he was contacted to give evidence for the 1st Petitioner based on the work he did on Aadhaar.

57. On re-examination by Mr. Waikwa, Counsel for the 1st Petitioner, Mr. Anand stated that the company he works for organizes technology conferences for technology practitioners. Further, that the papers presented in those conferences are in the computer science field. It was his view that the law should come before architectural design, noting that it is important to align projects to human rights. He contended that public confidence would be boosted where information on a project is in the public domain.

58. With regard to his contention in cross-examination that he knew what NIIMS was, he stated that he reached his opinion by considering its goals as set out in the pleadings of the Respondents, which showed that the system is centralised. According to Mr. Anand, a perusal of the data capture form disclosed that there were many other data bases by the number of identity documents required by the form. Further, as the system was going to link all the databases to the central database, it was a centralised and federated database linked to other functional databases.

59. Asked to define certain technical terms that he had used in his evidence, Mr. Anand stated that ‘enrolment’ is the process of giving personal information and biometrics for use in an identification system. Further, that ‘deduplication’ is an outcome in which no two entries should belong to the same person in a database, and every person should have only one entry in the database. He stated that ‘deduplication’ is a process of algorithms and thresholds that give a person an identity and links it with the system by giving the person a unique number for authentication.

60. Mr. Anand explained that multi-modal systems are used to achieve deduplication. He further explained that multi-modal systems combine data, whether biometric or otherwise, of

a person, and compare it with previous data and assign a unique number to the person. He stated that one could not get an identification number from NIIMS if the database indicated that there was another like person in the system.

61. With regard to the meaning of the term ‘deterministic,’ he stated that it meant that something was going to happen no matter what. On the other hand, that the term ‘probabilistic’ meant that it was not known for certain if something will happen. In Mr. Anand’s view, it was mathematically impossible to say that the NIIMS system will be deterministic as one can only set thresholds for each biometric parameter in order to determine identity.

62. Mr. Anand also described how databases are linked. He stated that the linking would require similar fields of entry across all the databases which are then connected. He noted that databases cannot be linked if they are not harmonised, a term which he defined to mean that structures are similar across all databases. On ‘identity’ and ‘identification’, he stated that ‘identity’ means giving legal recognition to a body that exists, whereas ‘identification’ is a process defined by a third party which confirms the identity of a person. In his view, NIIMS was an identification project as confirmed by statements made by the Respondents.

63. Mr. Anand stated that there was a possibility that people who had not enrolled would be rejected by the system as duplicates. He enumerated five concerns that he had in regard to NIIMS. The first was its purpose-free architecture, meaning that the data could be used for any purpose and has no limitation. On the other hand purpose-limited architecture requires the data to be used only for specified purposes.

64. His second concern related to the enrolment system design. He stated that the data capture form asked for detailed information which is not required for giving a person a unique identity number that in other words, there is no data minimisation. Thirdly, he was concerned that the system was exclusionary by its architecture and design in that citizens may be prevented from getting their rights by, for instance, the requirement that they must have an existing identity card or good quality biometrics in order to be registered in NIIMS.

65. The fourth concern related to fear of mass surveillance. He expressed the view that government is able to conduct surveillance of its citizens from the data it collects because it has the decryption key. Further, that such surveillance is also a possibility with respect to functional and subsidiary databases which are not encrypted. In addition, that commercial surveillance can also arise from profiling of persons using the data collected.

66. Mr. Anand’s fifth concern related to breaches of the system and fraud. He stated that even though the Respondents alleged that the data would be protected through encryption, data must be decrypted before use, leading to security risks. He stated that hacking occurs when data is used and the encrypted data in this respect will need to be used for authentication purposes thus raising the opportunity for hacking. Mr. Anand explained that fraud is committed for a specific purpose, mostly financial gain, and centralising data raises the benefits of hacking to the fraudsters.

67. Finally, he expressed the opinion that the NIIMS system is archaic and there was failure to consider modern designs and alternatives. He gave examples of alternatives as including removing the linkages to functional databases such as in Austria and Estonia, or the use of PIN-based cards to authenticate identity instead of biometrics.

68. Questioned about the use and implication of open versus closed source technology, Mr. Anand stated that an open source technology project is constantly being peer-reviewed by a larger community of digital experts, which makes it more robust. With respect to whether such a system will deter terrorism, he stated that because of the large number of people trying to fix any loophole in the system, there is disclosure about loopholes which is a way of preventing the loopholes being used. He stated that in relation to NIIMS, there is no documentation or knowledge on the design, and one could not therefore know what loopholes there were in NIIMS. He stressed that in India, the information on the design of Aadhaar was in the public domain and he had even identified the loopholes and informed the government about it.

69. Mr. Anand stated that a cost-benefit analysis ought to have been carried out prior to implementation. He reiterated that NIIMS, being a digital infrastructure project, required a detailed cost-benefit analysis, and there was no evidence of such a process in NIIMS, which he concluded was not a well-thought out project.

70. Answering questions put to him in re-examination by Mr. Awele for the 2nd Petitioner, Mr. Anand stated that NIIMS is not deterministic, and that for a system to be deterministic, one needed to collect a lot of personal data using a multi-modal identity system. He stressed that the State will have to have a lot of data points for the system to be deterministic. He acknowledged that the Respondents had indicated in their replies their preference for closed source software. He had not, however, seen the design and architecture of the NIIMS system, but his view was that the government should have disclosed information about its technical architecture and algorithms to illustrate the soundness of the design and open it to scrutiny.

71. In response to questions put to him by the Court, Mr. Anand stated that centralised databases usually hold a lot of information and the risk of such a system is twofold. First, the impact of a breach will be massive, and secondly, the risk of a breach is higher when there is a linkage between the central and functional databases. He explained that where there is no linkage between the functional and the central databases, the impact of a breach is reduced. He emphasised that this is why data minimisation is important and stated that only the data required for identification should be kept in the central database. He conceded, however, that the risks can be mitigated through the law, design architecture and technology.

72. Mr. Anand also expressed the view that the system architecture should not allow mass surveillance but may allow targeted surveillance, which should occur under judicial supervision or oversight processes. He accepted that there is no system that is immune to fraud but the impact can be minimised.

73. Mr. Ahmed Khalil Kafe testified as PW3. The evidence gleaned from his affidavit sworn on 12th April, 2019, is that he is a Kenyan citizen of Nubian descent born on 18th March 1946. He served as a police officer under the Kenya Police Force from 1965 to 1972, and that in 1968 he specifically served in the Presidential Escort. After retiring from the Police Service in 1972, he engaged in small-scale business in order to earn a livelihood. At around that time, he lost his identification documents namely an identification card, a driving licence and police card through a theft that occurred in his home. As required, he obtained a police abstract, but because of the size and the quality of the abstract issued at that time, it became worn out and eventually all the writings disappeared.

74. Mr. Kafe's testimony was that he made an application for the replacement of his national identification card on 19th November 2018. When he reached the fingerprint verification stage
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 14 of 205.

during the replacement process, he was informed that his fingerprints were not available in the records at the National Registration Bureau. He was then asked by the officials at the Office of the Registrar of Persons to swear an affidavit for the lost documents to facilitate the replacement of the national identification card. However, despite swearing two affidavits and following up on the matter, he had not obtained a national identity card. He deposed that it has been four years since he lost his documents and all his efforts to have replacements were constantly rendered futile. He stated that due to illness he had stopped following up on the documents and was thus unable to procure simple services like registration of a phone number, opening an M-pesa account, registration of a small business, or even to travel.

75. It was Mr. Kafe's closing statement that on 10th April, 2019 at the Makina Mosque in Kibera, he applied for the *Huduma Namba* but his efforts were rendered unfruitful by the officials who sent him away without attending to him.

76. When cross-examined by Mr. Nyamodi, Mr. Kafe told the court that his complaint was in regard to the difficulty of obtaining a national identity card. He confirmed that his national identity card got lost long ago, after he left the police force in 1972, and that he applied for the replacement of his identity card on 19th November, 2018.

77. On re-examination by Mr. Bashir, Mr. Kafe stated that he applied for his first identity card in 1961 or 1962, before independence. He confirmed that he had a waiting card with his photograph which was issued to him on 5th September 2019. His testimony was that his problem in this case is that without an identity card, he cannot get a *Huduma Namba*.

78. Mr. Shafi Ali Hussein, who identified himself as the Chairman of the Nubian Rights Forum, testified for the 1st Petitioner as PW4. His evidence as it emerged from his affidavits was that the NIIMS database would be linked with other official registries to form a single, government-mandated identity system. Further, that this system will be linked to the delivery of an undefined sphere of government services, including access to identification documents, universal healthcare, fertilizer subsidies, cash transfers, affordable housing and education.

79. Referring to a report titled **Statelessness and Citizenship in the East African Community** by the United Nation High Commission for Refugees dated September 2018, he stated that the Kenya Government continues to subject its citizens of Asian, Somali, and Muslim heritage to vetting procedures prior to issuing identity documents. While the vetting is intended to counteract fraudulent acquisition of documents, it was his averment that the same controls are not applied to other ethnic groups. He averred that this had resulted in many people in the targeted groups remaining without national identity cards.

80. Mr. Shafi averred that the current registration system for identity cards, which is a simpler system, has complications for residents in marginalized areas who cannot access services, either due to discrimination or lack of resources. Further, that the Registration of Persons Act allows for the establishment of "*identification committees*" by the Registrar for the purpose of "*authentication of information*", whose composition and nature is increasingly security-based, reflecting a widely observed trend towards systematic state surveillance of the population.

81. It was therefore Mr. Shafi's averment that since these historical issues have not been addressed, rolling out a more complicated process of registration will only serve to increase the difficulties. His view was that there is a danger of people from such communities being

left out of the registration, which will render them unable to access any public facilities, leading to discrimination in violation of the Constitution.

82. While referring to the *kipande* system which he termed as a “*diabolical system of fingerprints*”, Mr. Shafi deposed that the history of identity systems is that they are not universal but are used to monitor, exclude and even to assimilate or “*erase*” specific groups. He expressed the view that the capture of biometric information has also tended to intrude deeper into people’s lives during moments of crisis, actual or perceived, and to target specific groups on the basis of ethnicity. He cited as an example the fact that during the Mau emergency period, the authorities began collecting full fingerprints as opposed to just a single digit or thumbprint, imposing this new system on all “*members of the Kikuyu and allied tribes.*” He cited in support an article by Keith Breckenridge titled **The Failure of the “Single Source of Truth about Kenyans” : The National Digital Registry System, Collateral Mysteries and the Safaricom monopoly** dated 23rd August 2017.

83. Mr. Shafi averred that Kenya’s civil registration system has been harshly criticized by international institutions like the African Commission on Human and Peoples’ Rights and the United Nations Committee on Elimination of Racial Discrimination (CERD), as well as national bodies, such as the Truth, Justice and Reconciliation Commission (TJRC), the Ethics and Anti-Corruption Commission and the Commission on the Administration of Justice. Further, that the discriminatory impact of identity registration practices in Kenya upon national minorities has also faced criticism. He cited the TJRC report as demonstrating that Muslims in particular “*suffered discrimination for decades in relation to their right to citizenship and associated identity documents.*”

84. Turning specifically to the Kenyan Nubian community, Mr. Shafi averred that the community had filed complaints with the African Union institutions in the cases of **Nubian Community in Kenya vs Kenya** and **Children of Nubian Descent in Kenya vs Kenya** in which decisions were rendered that found Kenya’s registration and identity documentation practices discriminatory and infringed the rights of members of the community. Further, that specific recommendations were made to the Kenyan government to cure the violations.

85. Relying on a study carried out by the Open Society Foundation in 2015 titled **Legal Identity in the 2030 Agenda for Sustainable Development: Lessons from Kibera** Mr. Shafi averred that empirical research has confirmed that inability to access documentation of citizenship in Kenya results in serious restrictions on one’s ability to enjoy rights and freedoms guaranteed in the Constitution and international and regional human rights instruments. According to Mr. Shafi, the study revealed that “*in Kenya a national identity card issued at age 18, rather than a birth certificate, is the necessary document to access many services and exercise rights.*”

86. Mr. Shafi stated there are several questions regarding the impugned statutory amendments, as there are no clear provisions indicating how the process of data collection shall be done, and no specific reason given for the collection and use of the private data. Further, that there is no provision on how one can amend the data once it is collected, which can lead to people being locked out from accessing government services because of wrong data. In addition, that the data to be collected is personal and private, and mishandling of the same shall amount to grave breach of the right to privacy, among other rights.

87. Mr. Shafi stated that IDEMIA (previously or concurrently operating as Morpho/OT-Morpho/Safran Identity and Security) is the company awarded the contract to build the
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 16 of 205.

NIIMS system. It was his evidence that this was the same company contracted to develop the voter registration system in the 2017 General Election known as Kenya Integrated Election Management System (KIEMS). He contended that the data contained in KIEMS was compromised, the implication being that IDEMIA could not be relied upon to develop NIIMS. Furthermore, that there is no public record on when the tender for NIIMS was floated, which companies applied, the selection process and the decision. Further, that he had not seen any public record on any due diligence carried out to ensure the privacy of the information collected by IDEMIA.

88. While reiterating his claim that IDEMIA is unreliable, Mr. Shafi averred that the same entity was contracted by the Ghanaian government to collect data, print identity cards, and manage the system, but that when its contract was terminated it refused to release the registration data to the government until payment was made. This, in his view, put at risk the right to privacy.

89. Mr. Shafi further averred that the right to privacy was threatened with violation by the fact that there are no proper data protection laws in place to guarantee privacy. In addition, that no mention is made with respect to who exactly can access the data and for what purpose, leaving an opening for unauthorized persons to access the sensitive data. Further, that the World Bank in its 2016 report titled ID4D Country Diagnostic: Kenya advised that the national legal framework for registration and identification should be strengthened “*around data protection and privacy*”, and had made detailed comments on the weaknesses of the Data Protection Bill.

90. Referring to the African Union Commission’s Personal Data Protection Guidelines for Africa, Mr. Shafi averred that the principles for data protection include consent and legitimacy, fair and lawful processing, purpose and relevance of data, management of the data lifecycle, transparency of processing and confidentiality and security of personal data. It was his deposition that the impugned legislation does not comply with the said core data protection principles.

91. Mr. Shafi faulted the Respondents for rolling out NIIMS without benchmarking with developed and well-known systems such as Aadhaar in India. Citing the State of Aadhaar Report 2017-18 dated May 2018, he averred that the Aadhaar system was introduced in India to provide identification to citizens and residents, and its processes were relatively similar to the NIIMS system. His evidence was that the Aadhaar system has reported more errors than benefits. Further, that the report established that nearly two million people in three Indian states were excluded from accessing food subsidies as a result of Aadhaar-related factors. He further contended that India has also struggled with ensuring data security. He cited in this regard a report by the Center for Internet and Society (CIS) which had revealed that the Indian government inadvertently published the biographic and demographic data linked with Aadhaar numbers on 135 million Indians on the open internet. In his view, there is a possibility of Kenya facing the same problem in different ways.

92. Mr. Shafi also expressed the fear that just like in India, the data in NIIMS may be used for personal benefit. He averred that Aadhaar is the subject of dozens of lawsuits in Indian courts, and the Supreme Court of India has restricted the linkage of private sector services to Aadhaar enrolment; limited the mandatory use of Aadhaar for delivery of government services; permitted children to opt out of the system entirely until they turn 18; mandated an effective redress mechanism when data is misused; minimised the kind of data the

government is permitted to collect; and reduced the storage period for authentication logs from 5 years to 6 months.

93. In Mr. Shafi's view, the introduction of NIIMS in a legal and regulatory context in which ethnic and religious discrimination prevents minorities like the Nubians from accessing identity documents exacerbates their discrimination without any reasonable justification. He asserted that the effect of rolling out the system will defeat the stated purpose of NIIMS, which is to provide universal access to government benefits, services and the digital economy.

94. Mr. Shafi explained the context in which he wrote a letter dated 8th April, 2017 in his further affidavit sworn on 12th April, 2019. He stated that the letter was a response to a mobile identity card registration campaign carried out by the 2nd and 3rd Respondents. His explanation was that the letter illustrated that the Nubian community has faced discrimination, hence the need for special registration initiatives. Further, that the appreciation by the 1st Petitioner in the said letter of the work of the National Registration Bureau did not mean that the discrimination against the Nubian community has ceased, but merely signified the 1st Petitioner's goodwill and cooperation.

95. Mr. Shafi deposed that the plight of the Nubian community with respect to registration of persons was not unknown to the 2nd Respondent and its respective agencies. This was because it was an issue in the case of **The Nubian Community in Kenya vs The Republic of Kenya** at the African Court on Human and Peoples' Rights. His testimony was that the requirement for a national identity card number in the NIIMS enrolment form was meant to target the members of the Nubian community who do not have such details because of the numerous vetting processes conducted by the 2nd Respondent.

96. Mr. Shafi stated that the NIIMS enrolment form clearly indicated that a *Huduma Namba* was a mandatory requirement for receipt of all services, and this would expand the scope of discrimination already suffered by the Nubians. He deposed that he had personally witnessed a significant number of members of the Nubian community being turned away for lack of various requirements like the identification card during the NIIMS pilot project phase launched on 15th February 2019. It was his averment that the registration for NIIMS was mandatory, and hence violated the spirit of Article 31 of the Constitution.

97. Referring to the disclaimer in the NIIMS enrolment form which stated that the data may be shared with third parties, Mr. Shafi reiterated that there is no comprehensive data protection framework in Kenya. His opinion was that the enactment of the data protection laws should have preceded the NIIMS registration process.

98. When cross-examined by Mr. Nyamodi for the 4th and 7th Respondents, Mr. Shafi stated that at the time he swore his supporting affidavit on 14th February 2019, the NIIMS enrolment exercise had not commenced, but could not remember whether the enrolment had started by the time he swore his further affidavit on 12th April, 2019. He did not respond to the question whether he had, in his affidavit, indicated the provisions of the Constitution that had been violated.

99. Mr. Shafi stated that the issue of vetting procedures prior to the issuance of identity documents preceded NIIMS. His testimony was that his problem with the vetting committees was that they were becoming more security-based. He conceded that the vetting procedure is provided for by section 8(1A) of the Registration of Persons Act, and that an elder of the Nubian community is a member of the vetting committee. His view, however, was that the

issues of discrimination in the vetting process have not been addressed, though he disclosed that he had not personally been vetted for purposes of obtaining a passport, nor had he ever been a member of a vetting committee.

100. Mr. Shafi further conceded that although he had averred that there were no clear provisions indicating how the data collection was to be done, he had not enrolled for the *Huduma Namba*, and had no experience on how the data was collected.

101. When asked about his averments regarding the process of procurement for NIIMS, Mr. Shafi indicated that he was not familiar with the procurement processes but was aware of the Procurement Act. He conceded further that procurement was not raised as an issue in the 1st Petitioner's petition but asserted that they searched for information on the procurement for NIIMS on the government domain. He insisted that the information for the *Huduma Namba* was collected by IDEMIA, and that this was the same company which was contracted by the Independent Electoral and Boundaries Commission during the elections.

102. When shown an averment by Jerome Ochieng on behalf of the 5th Respondent that no private entity, including IDEMIA, was used to develop the software for NIIMS, he stated that he did not remember if he had specifically responded to that particular statement. When confronted with the averment by the said deponent that benchmarking trips were made to countries with similar systems, he could not defend his allegation that the Respondents failed to compare the system with other systems such as Aadhaar in India.

103. When shown a copy of the letter he wrote dated 8th April 2017 referenced "*Appreciation Letter*" and addressed to the 4th Respondent, he asserted that the letter did not reflect the sentiments of the Nubian community about the issuance of identity cards.

104. On re-examination, Mr. Shafi stated that he wrote the letter dated 8th April 2017 to appreciate a good deed, as there is normally a problem between civil society and government. Further, that he had written the letter on behalf of the 1st Petitioner which was partnering with the Registrar of Persons and mobilizing the residents in the issuance of identity cards and birth certificates. He stated that his only problem with the vetting process was that it is only specific communities that are vetted.

105. Mr. Shafi named the members of the vetting committee as the Registrar of Persons, Registrar of Births and Deaths, a District Commissioner or District Officer, an intelligence officer, a senior police officer, an officer from the Directorate of Criminal Investigation, and one Nubian elder. That other than the one Nubian member, the rest of the members are government officials.

106. Mr. Shafi clarified that his grievance with NIIMS and *Huduma Namba* was that members of the Nubian community would be left out of the exercise. He urged that the issues of discrimination should first be addressed, so that Nubians can walk together with other Kenyans in the NIIMS project.

107. Ms. Fatuma Abdulrahman, who identified herself as a member of the Nubian community, testified as PW5. In her affidavit sworn on 12th April 2019, she gave a background to the challenges facing the Nubian community. She stated that there was no significant discrimination against the community prior to 1990, and they accessed identity documents like other Kenyans. From the 1990's, however, they started facing severe challenges in accessing documentation and were subjected to differential treatment in terms of access to birth certificates, national identity cards, and passports. They also started

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 19 of 205.

experiencing delays in the issuance of documentations and rejection of documentation without any justifiable reasons. In her view, these challenges coincided with their aggressive quest for the Kibra land in Nairobi, and the new generation of Nubians started being branded non-Kenyans. Her opinion was that this was a strategy of disinheritance of their children from the Kibra land.

108. Ms. Abdulrahman testified that the differential treatment further worsened after the 7th August 1998 bomb attack and subsequent terrorist attacks in Kenya. She stated that at this juncture, some minority groups like the Nubian community were profiled as a security threat, and had to undergo extra scrutiny or vetting to prove that they are Kenyans. She asserted that the security vetting intensified after its legalisation in the Security Laws Amendments Act 2014.

109. In her view, the security vetting results in many Nubians experiencing extreme delays in their applications for documentation, or going without documentation. Further, that the delays result in missed educational, employment and other opportunities. According to Ms. Abdulrahman, this profiling has been detrimental to the community, and has also caused clashes and tension between its members and neighbouring communities, and she gave the example of the ethnic clashes in Kibra in 2001.

110. Ms. Abdulrahman testified that due to the challenges the community faced, it had tried to seek legal redress in the High Court of Kenya but was unsuccessful. It had then moved to the regional level to get a remedy, and she cited the two decisions of the African Commission on Human and Peoples' Rights and the African Committee of Experts on the Rights and Welfare of the Child (ACERWC) referred to in the 1st Petitioner's Petition. The two cases had been resolved in favour of the community.

111. Ms. Abdulrahman's deposition was that despite the decisions and the fact that international law is part of Kenyan law, the government is yet to implement the recommendations in the two decisions. It was her evidence that some discriminatory practices had in fact become more severe, and included increased requests for supporting documents, as well as the introduction of a requirement of an applicant's parent's thumb print on an identity card application form.

112. Ms. Abdulrahman also narrated in detail the steps taken by the 1st Petitioner to improve access to government documentation by her community. It was her testimony that over 3,200 people had been assisted to apply for birth certificates, identity cards, passports, and death certificates. She stated that Nubians in Kibra are only able to apply for identity cards on Tuesdays or Thursdays, as these are the days that the vetting committees sit. Further, that a Nubian applicant must first provide their documentation to Nubian elders for review and for signing of an affidavit that confirms that the elders know the applicant as a member of the Nubian community. She went on to explain the vetting process at length, and presented what she termed empirical findings and observations on the time taken and delays in applications for documentation by members of the Nubian community.

113. In cross-examination by Mr. Nyamodi for the 4th and 7th Respondents, Ms. Abdulrahman clarified that she is an official of the 1st Petitioner working on citizenship rights issues for the Nubians. It was her testimony that the 1st Petitioner was in court because the Nubian community experiences difficulties in getting documents such as identity cards, passports and birth certificates, which are used in the *Huduma Namba* registration.

114. In re-examination by Mr. Bashir, she expounded on the decisions they obtained from the regional bodies and stressed the challenges that a Nubian child undergoes before getting an identity card. In her view, the difficulty in obtaining documents would make it difficult to register for the *Huduma Namba*.

115. The 1st Petitioner also filed an affidavit sworn on 11th April 2019 by Dr. Thomas Fisher, a Research Officer with Privacy International since February 2016. Dr. Fisher averred that he swore the affidavit on behalf of Privacy International, a non-profit, non-governmental organisation based in London and established in 1990, which has been working on issues relating to identification systems. His affidavit was intended to provide expert evidence in support of the 1st Petitioner's case.

116. It was his deposition, on the basis of various articles in international instruments, that the right to privacy is a fundamental right enshrined in many constitutions around the world, as well as in international human rights law. He noted that as early as 1988, the UN Human Rights Committee had recognised the need for data protection laws to safeguard the fundamental right to privacy.

117. Dr. Fisher averred that his organisation had noted concerns with identity systems around the world. In his view, some of the concerns can be partially mitigated by legal, procedural and technological safeguards, as explained by the World Bank ID4D initiative in its publication titled *Principles on Identification for Sustainable Development: Toward the Digital Age* (2017). Further, that these mitigations should be implemented at the design stage, rather than later, in order to ensure that privacy is embedded at the outset into the systems. He was of the view, however, that mitigations cannot solve all problems with identity systems, and challenges still remain.

118. Dr. Fisher's affidavit focused on identity systems that use biometrics and unique identifiers. He defined the term biometrics as the measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals. He gave examples of the modalities that can be used to include fingerprints, iris, facial photographs, and vein patterns and explained the processes involved in extracting, storing and using biometrics.

119. Dr. Fisher addressed various challenges that arise with biometric databases. He referred to the report by the United Nations High Commissioner for Human Rights (UNHCR) on **The Right to Privacy in The Digital Age** dated 3rd August 2018 and the report by the European Union Agency for Fundamental Rights titled **Fundamental Rights Implications of Storing Biometric Data in Identity Documents and Residence**

120. **Cards**, (2018) which highlight significant human rights concerns with the creation of mass and centralized databases of biometric data. According to these reports, due to the scale and sensitive nature of the data which is stored, the consequences of any data breach could seriously harm a potentially large number of individuals. Further, that if such information fell into the wrong hands, the database could become a dangerous tool against fundamental rights.

121. Dr. Fisher further deposed that some individuals may have biometric features that make it challenging or impossible to enrol or authenticate them, citing the case of manual labourers who may have worn fingerprints. It was also his deposition that in some occasions, it may be inappropriate and an invasion of an individual's privacy to collect facial photographs, for example for those who wear headgear for religious reasons, or are part of communities who

object to having their photographs taken. His averment therefore was that enrolling in a biometric system can be physically impossible or privacy invasive.

122. Another challenge identified by Dr. Fisher is that biometrics can potentially be used to identify an individual for their entire lifetime. This means that caution has to be shown in the face of changing regimes or political contexts, and also the changes in technology. The technology surrounding biometrics is continually evolving, which places new pressures and risks on biometric systems. For example, it is possible to clone a fingerprint from a photograph, using commercially-available software. Another concern identified by Dr. Fisher is that unlike a password, an individual's biometrics cannot be changed.

123. A further challenge identified by Dr. Fisher is that biometrics are essentially probabilistic and there are other means of authenticating the individual that are deterministic. He gave the example of the use of Personal Identification Numbers (PIN), which either matches or does not match with the stored PIN. He deposed that biometrics are different and do not make a definitive decision on whether an individual is who he or she claims to be, but rather a probabilistic one. This meant, according to Dr. Fisher, that some individuals are going to be excluded from what they are entitled to, or falsely accepted as somebody they are not.

124. Dr. Fisher also addressed the challenges arising from the use of unique identifiers. He defined a unique identifier as a unique number or code, for example an identity number. He stated that a unique identifier is a feature of an identity system that is particularly problematic, arising from the 'seeding' of identity numbers across multiple government or private sector databases. This, he stated, creates the risk of providing a "360 degree view" of an individual. His evidence was that the linking and seeding of databases with a single number gives the opportunity for all information about an individual, across multiple databases, to be accessed. Citing a statement in the United Kingdom case of Marcel vs Commissioner of Police of the Metropolis [1992] Ch 225 (Browne- Wilkinson VC), he contended that the gathering of information about an individual from several government agencies in one database places his or her freedom at risk.

125. Dr. Fisher observed that dangers also exist in the use of unique identifiers by the private sector, as it can lead to the exploitation of individuals and their data. He referred to a report by the London School of Economics titled The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications (2005), for the proposition that service providers can profile individuals who interact with them using electronic identifiers. He also cited the ruling of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others Writ Petition (Civil) No. 494 of 2012 where a section of the Aadhaar Act that allowed private companies to use Aadhaar authentication was declared unconstitutional. The Court had held that allowing private entities to use Aadhaar numbers will lead to commercial exploitation of individuals' personal data without their consent, and could lead to individual profiling.

126. Dr. Fisher averred that there are also new opportunities for fraud presented by the use of unique identifiers, particularly an identity number with a broad purpose which present more opportunities for a malicious actor to act fraudulently. He averred that an identity number with limited purposes limits the harms that can be caused to the individual.

127. Dr. Fisher identified some of the concerns that arise in relation to identity systems that use biometrics and unique identifiers exclusion, including data breaches, mission creep, access to and retention of data, and data protection. In his opinion, the above considerations

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 22 of 205.

are especially valid as regards the protection of special categories of more sensitive data and more particularly of DNA information. He also noted the need to place limitations on access by law enforcement and intelligence services to identification databases.

128. Dr. Fisher made averments with regard to the importance and necessity of data protection. He averred that as of January 2019, over 120 countries had enacted comprehensive data protection legislation, and many other countries were in the process of doing so. In addition, frameworks and instruments for data protection have been introduced by international and regional institutions such as the African Union, the Organisation for Economic Cooperation and Development, and the Council of Europe. In his view, data protection is necessary to safeguard the fundamental right to privacy by regulating the processing of personal data, providing individuals with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

129. Dr. Fisher averred that although a strong comprehensive data protection law will not cure the concerns he had identified, it is an essential safeguard in the introduction of any identity system. He identified the core principles for safeguarding of data that should be contained in data protection laws.

130. Dr. Fisher made averments with respect to mitigation measures that could be taken in order to protect data. He noted that in recognition of the particular concerns raised on the use of biometrics, consideration should be given to whether the stated purpose could be achieved by a less intrusive approach. Further, that use of data requires legal, procedural and technical safeguards. He cited the recommendation of the High Commissioner for Human Rights that States should ensure that data-intensive systems are only deployed when, demonstrably, they are necessary and proportionate to achieve a legitimate aim. He further cited the **U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179** (17 December 2018) which recommended that in collecting, processing, sharing and storing sensitive biometric information from individuals, States must respect their human rights obligations, especially the right to privacy. This should be done by the adoption of data protection policies and safeguards.

131. A second mitigation measure proposed by Dr. Fisher is avoiding storing the biometric templates in a centralised database. He asserted that this may avoid the risks of a system being used for identification, rather than just authentication. He recommended the use of a smartcard alternative to a centralised database, citing the UK's biometric passport as an example. He further averred that designing systems without a centralised database also reduces the risk of a major breach of biometric data.

132. Dr. Fisher expressed the opinion that a unique, single, persistent identifier or 'identity number' for citizens is not necessary for an identity system. He gave illustrations from the UK's *Verify.gov* system which does not require a single, unique identity number for individuals to authenticate their identities; Germany where the law prohibits the use of a unique identification number of general application; and India where, since the launch of Aadhaar in 2009, the system has undergone design changes that include the introduction of virtual identity and tokenisation as alternatives to the use of Aadhaar numbers to access services.

133. Dr. Fisher also cited the situation in Singapore in which a single identifier is used and can potentially unlock large amounts of information relating to the individual. This poses the

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 23 of 205.

risks of identity fraud and theft, and as a result, the data protection authority in Singapore prohibits the collection, use, or disclosure of the single identity numbers by non-public sector organisations, except when required by law or when it is necessary to identify individuals to a high level of fidelity.

134. Finally, Dr. Fisher observed that the Estonian system involves a platform known as X-Road that allows institutions to exchange data. However, the system also allows citizens to monitor how their data has been used by government departments since a log record is created whenever an individual's data is accessed.

The 2nd Petitioner's Case

135. The 2nd Petitioner, Kenya Human Rights Commission (KHRC), is a non-governmental human rights organization registered in Kenya on 20th January 1994. Its mandate is to *inter alia* secure human rights in states and societies through fostering human rights, democratic values, human dignity and social justice. The 2nd Petitioner filed a petition dated 18th February 2019, supported by an affidavit and a further affidavit of George Kegoro, its Executive Director, sworn on 18th February 2019 and 12th April 2019 respectively.

136. The 2nd Petitioner also relied on affidavits sworn on 12th April 2019 by its Deputy Executive Director, Davis Malombe, and by Alice Munyua, a Policy Adviser of the Mozilla Corporation. It also filed a witness affidavit dated 12th April 2019 by Grace Mutung'u, an Advocate of the High Court of Kenya, who was called to testify as an expert witness.

137. The 2nd Petitioner impugns the Act on four main grounds. The first is that there was a denial of the right to public participation in the process of enactment of the impugned amendments. The 2nd Petitioner avers that neither it nor the public were given a reasonable opportunity to comment on or contribute to the substantive provisions of the amendments at any stage prior to their passage by the National Assembly. Further, that any engagements with the public concerning the impugned amendments, if at all, were a wholly cosmetic public relation exercise designed to create the false impression of constitutional compliance.

138. It was further averred that the impugned amendments significantly alter the process of acquiring vital identity documents, which will impact every sphere of the day to day lives of Kenyans, and by extension, have far reaching consequences on the enjoyment of fundamental rights and freedoms. It contended therefore, that it would have been fair, just and in the public interest that the amendments be subjected to public participation, which did not happen in this case.

139. The 2nd Petitioner was aggrieved, secondly, by the enactment of the impugned amendments through an omnibus statute. It averred that it is a universally settled precept that substantive amendments with far-reaching consequences such as the instant ones should be effected through a substantive Act and not through a miscellaneous amendment in an omnibus Act. Consequently, that it was inappropriate and contrary to public interest to enact the impugned amendments vide an omnibus Miscellaneous Amendment Act. It contended that this concern was brought to the attention of the National Assembly on 28th August 2018 but was ignored. The 2nd Petitioner therefore takes the view that the impugned amendments were enacted into law vide an omnibus Bill to avoid scrutiny or for extraneous purposes.

140. The 2nd Petitioner's third concern relates to the security of the data collected under NIIMS, and citizens' rights to privacy. It averred that the impugned amendments impose extensive and unlimited mandatory requirements for citizens' personal information without

concomitant safeguards to prevent abuse or intrusions into people's privacy by the State or unintended third parties. It was its case that integrating all personal information of the population in one system, whose security and integrity has not been guaranteed by the law, will expose citizens to unimaginable risks should the system be compromised or breached in any way.

141. According to the 2nd Petitioner, the impugned amendments grant the relevant Cabinet and Principal Secretaries extensive powers to gather personal information and to make regulations with regard thereto without substantive framework limitations on the use of the information gathered, or the principles and standards that should be applied in the exercise of the said powers, contrary to Article 94(6) of the Constitution. Further, that these dangers are compounded by the lack of a policy and legal framework for data privacy and protection in Kenya. The 2nd Petitioner contended that the impugned amendments fall short of the United Nations Principles on Personal Data Protection and Privacy, the African Union Convention on Cyber Security and Personal Data Protection, as well as comparable laws from other jurisdictions on limitations to the right to privacy.

142. Lastly the 2nd Petitioner challenged the substantive provisions introduced by the impugned amendments in sections 3 and 9A(2) of the Act and contended that they are intrusive, ambiguous and susceptible to abuse. It set out the legal and operational shortcomings of the amendments under various limbs.

143. The first limb was that the said provisions require, in mandatory and unqualified terms, that all Kenyan citizens, including children, submit their personal information including DNA information without their consent to the State, thereby creating a national population register. Further, that this personal information is susceptible to abuse to advance commercial interests and exposes citizens to negative profiling, which may have serious implications for civil liberties.

144. The second limb relates to the amendments introducing a unique identification number linked to a central access platform that will be assigned to every person. The 2nd Petitioner contended that this will exacerbate the risk of compromise of the system, and by extension, the privacy and security of the people. In addition, that the impugned amendments do not provide for the transitional mechanism from the current registration regime.

145. It was its contention that moreover, persons locked out from registration for any reason risk being left out permanently without access to vital government services necessary for the fulfillment and enjoyment of fundamental rights and freedoms. The 2nd Petitioner noted that it was not opposed to the proposal that citizens be assigned unique national identification numbers, but was concerned with the security and integrity of the system.

146. The third limb particularized by the 2nd Petitioner is on the harmonization of personal information across government databases, which will entail information sharing among different agencies. It was contended that this exposes the NIIMS system to greater risks of intrusion and abuse since the amendments do not specify the operational linkages of the system with the other databases. The 2nd Petitioner contended that in any event there exists a parallel Integrated Population Registration System (IPRS) under the Kenya Citizens and Foreign National Management Service Act No. 12 of 2012 that duplicates the functions of NIIMS.

147. It was its contention further that the harmonization process is prone to breaches such as destruction, deletion or loss of vital records; identity theft and fraud; malicious use of the information, wrongful entries; and mismatch of information and hacks through cybercrimes, as it is currently not clear which institution or person will be accountable for the registration process.

148. Fourthly, the 2nd Petitioner impugned the provisions on verification and authentication of information relating to identification of persons. It contended that NIIMS is only capable of verifying and authenticating documents issued by it, and the impugned amendments do not therefore provide for mechanisms for inter-agency or inter-governmental cooperation necessary to support the function of verification and authentication. Its view was that the power of authentication of personal information is left to one system, without checks and counter-checks, thereby negating the principle of accountability.

149. The fifth challenge to the impugned amendments related to the question of access to the data. The 2nd Petitioner contended that the provisions on collation of information does not specify any limitations on the circumstances and/or persons to whom personal information may be shared, making it possible to share citizens' personal information with third parties, including foreign States.

150. In its sixth limb, the 2nd Petitioner contends that section 9A (2)(h) of the Act does not contemplate or prescribe any consequences or penalty in law for unauthorized or accidental access, damage, loss or other risks presented by the proposed system. It was its case further that it also fails to guarantee protection of personal information from unscrupulous and corrupt officers, nor does it set immutable standards that the system must comply with in order to protect personal data.

151. The 2nd Petitioner contends, lastly, that section 9A (2)(i) affords 'any person' the right to apply for rectification of 'any errors' in the register instead of restricting it to the owner of the information only. It contends that the State cannot, on its own initiative, determine what is or is not accurate, complete or up to date and not misleading information. The 2nd Petitioner contended that the State should accordingly specify the applicable standards and principles of amendment of information, for example by defining the scope and nature of personal information required under the Act. Its view was that this would make it possible to anticipate with reasonable certainty whether an amendment is necessary and what 'complete', 'up to date' and/or 'not misleading' information is.

152. The 2nd Petitioner therefore seeks the following orders:

a) A declaration that the amendments to the Registration of Persons Act, Cap 107 Laws of Kenya, vide the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018 are unconstitutional null and void.

b) A declaration that the amendments to the Registration of Persons Act, Cap 107 Laws of Kenya, by the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018 were enacted unprocedurally and without public participation contrary to Articles 10(2)(a) and 118(1)(b) of the Constitution.

c) A declaration that the amendments to the Registration of Persons Act, Cap 107 Laws of Kenya, by the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018 are inconsistent with the Bill of Rights and are unconstitutional null and void.

d) A declaration that the amendments made to the Registration of Persons Act, Cap 107 Laws of Kenya, by the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018 are otherwise unreasonable and unjustifiable in an open and democratic society based on human dignity, equality and freedom, contrary to Article 24(1) of the Constitution.

e) An order prohibiting the Respondents, by themselves, their employees, agents and or servants from installing and operationalizing the National Integrated Information Management System in any manner howsoever until policy, legal and institutional frameworks compliant with the Constitution are put in place.

f) Any other orders and/or reliefs as the court may deem fit.

g) Costs of the petition.

The 2nd Petitioner's Evidence

153. In his supporting and further affidavits Mr. George Kegoro reiterated the contents in the Petition with respect to the enactment and effect of the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018. He averred that unless the orders sought in the 2nd Petitioner's Petition are granted, the substantive objects of the said amendments shall seriously dilute fundamental rights and freedoms protected under the Bill of Rights, or subject them to serious threats of violation by the State and or unintended third parties. He listed five reasons why the amendments to the Act and the establishment of NIIMS violated or pose a threat of violation of fundamental rights and freedoms.

154. The first reason pertains to the threat of violation of the right to privacy and associated rights. Mr. Kegoro averred that any interference with the Bill of Rights amounts to a collateral attack on the dignity and potential of the people. It was his averment that in the digital age, personal information is vital data. Consequently, integrating all personal information of the population of Kenya in one system whose security and integrity has not been guaranteed by the force of law will expose citizens to unimaginable risks should the system be compromised or breached in any way. The result of such breach would, in his view, be to disrupt or curtail, in material respects, the enjoyment of almost all fundamental rights and freedoms under the Bill of Rights.

155. According to Mr. Kegoro, the impugned amendments of the Act impose excessive and unnecessarily extensive mandatory requirements for citizens' personal information without providing for concomitant safeguards to prevent abuse or intrusions by the state or unintended third parties. The effect of the amendments would be to breach Article 31(c) of the Constitution that guarantees every person the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed.

156. Mr. Kegoro averred that in view of the stated functions set out in sections 3 and 9A (2)(c) and (d), the impugned amendments are bound to impact every aspect of people's lives including access to the right to education and health as well as related services, the 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, human dignity. In his view, since the impugned amendments do not specify how sensitive personal information will be collected, verified, stored, secured, accessed and utilized, there is real threat that the system is susceptible to breach, which would occasion irreparable harm

and damage to the people and the country at large. He attributed this danger to the fact that Kenya does not have legislation or policy on data protection.

157. Mr. Kegoro further averred that in his view, the impugned amendments are almost certainly *ultra vires* the standards of limitation of fundamental rights set out in Article 24(1) of the Constitution. He averred that as a matter of fact, the amendments ostensibly repeal Article 31(c) of the Constitution.

158. The second reason advanced by Mr. Kegoro is that the amendments have elementary law defects, ambiguity and susceptibility. He cited in this regard sections 3 and 9A (2) of the impugned Act which he termed particularly intrusive, ambiguous and susceptible to abuse. He then proceeded to point out the shortcomings of each of the sub-sections of section 9A (2) of the impugned Act.

159. With regard to section 9A (2)(a) which creates NIIMS, he averred that the provision requires, in mandatory and unqualified terms, that all Kenyan citizens, including children, submit their personal information to the State. He contended that the section does not define what constitutes ‘personal information’, or the applicable standards and principles to be observed in gathering the said information including where, when and how the said information may be gathered and by whom. He further contended that in essence, the provision permits the State to require all manner of private information, including DNA, from citizens without their consent.

160. Mr. Kegoro averred, on the basis of advice from various experts and his own knowledge obtained from various research papers on the subject, that DNA information can be used for a variety of purposes which makes it susceptible to abuse and exposes citizens to negative profiling. It was his view that such negative profiling would have serious implications for civil liberties and could allow the State or unintended third parties to compile files containing highly personal data such as a person’s racial origins, medical history or psychological profile. He averred that such information can be abused by the State to suppress civil liberties or by business enterprises to advance commercial interests without the subject persons’ consent.

161. It was his further averment that the impugned amendments also purport to confer functions ordinarily performed by a legal person, usually a legal officer or corporation, on a system. In his view, this essentially renders the system supreme and unquestionable and thereby yields control of sensitive personal information to the inventor or author of the system.

162. With respect to section 9A (2)(b) which provides for the assignment of a unique national identification number to every registered person, Mr. Kegoro averred that the 2nd Petitioner was not, in principle, opposed to the assignment of such a number to citizens. He averred, however, that unless the concerns regarding the security and integrity of the system were addressed, a unique identification number as a central access platform will exacerbate the risk of compromise of the system and, by extension, the privacy and security of the people.

163. It was his averment further that persons locked out from registration for any reason risked being left out permanently without access to vital government services necessary for the fulfilment and enjoyment of fundamental rights. This, in his view, would be inconsistent with Articles 12(2) and 24 of the Constitution. He also contended that the impugned Act does not provide for transitional mechanisms from the current registration regime. There was no

indication, for instance, as to when the unique identification number will be issued in the current roll out phase. In his view, this lacuna exposes citizens to unfair inconveniences that may be occasioned by whimsical administrative orders or directives for the implementation of the system.

164. The 2nd Petitioner also challenged the provisions of section 9A (2)(c) of the impugned Act. This provision requires the harmonisation, incorporation and collation into the register of all information from other databases in government agencies relating to registration of persons. Mr. Kegoro averred that such harmonisation entails information sharing amongst different agencies, which exposes the system to greater risks of intrusion and abuse. He averred that the amendments do not specify the interoperability modalities of the system. This was so, in his view, particularly in light of the fact that there currently exists a parallel Integrated Population Registration System (IPRS) under the Kenya Citizens and Foreign National Management Service Act No. 12 of 2012 which essentially duplicates the functions of NIIMS. According to Mr. Kegoro, the harmonisation process is prone to breaches as it is currently not clear which institution or person under the impugned Act and the Kenya Citizens and Foreign National Management Service Act will be accountable for the registration process.

165. Mr. Kegoro averred that the breaches in the harmonisation process could include destruction, deletion or loss of vital records, identity theft and fraud, malicious use of the information, wrongful entries, mismatch of information and hacks through cybercrimes. In his view, there would be no prejudice occasioned to any party if all these duplications and mismatches are harmonised in law before the system is operationalised.

166. The 2nd Petitioner further impugns the provisions of section 9A (2)(f) which relates to the verification and authentication of information relating to the registration and identification of persons. Mr. Kegoro averred that NIIMS is only capable of verifying and authenticating documents issued by itself. He contended that the amendment does not therefore provide for mechanisms for inter-agency or inter-governmental cooperation necessary to support the function of verification and authentication. It was his deposition that this failure negates the principle of accountability as it vests the power of authentication of personal information on one system without checks and counter-checks.

167. With regard to the provisions of section 9A (2)(g) which provides for the collation of information obtained under the Act and its reproduction, as required, from time to time, Mr. Kegoro averred that the provision lacks in specificity. He contended that the authority to 'collate' and 'reproduce' essentially presupposes discretion to manipulate personal information to suit varying circumstances at the State's convenience. He averred that the provision does not specify any limitations on the circumstances or the persons to whom personal information may be shared. In his view, this makes it possible to share, without notice, citizen's personal information with third parties, including foreign States and private business enterprises that would otherwise not be entitled to access such information.

168. The 2nd Petitioner also impugns the provisions of section 9A(2)(h) of the Act. This section provides that NIIMS shall ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register. Its grievance with respect to this provision is that it does not contemplate or prescribe any consequences or penalty in law for unauthorized or accidental access, damage, loss or other risks presented by the proposed system. It was Mr. Kegoro's averment that weighed against the nature and

importance of the right to privacy, the provision is inadequate to guarantee the protection of personal information from unscrupulous and corrupt officers given the accountability loopholes identified in the system. The 2nd Petitioner's position is that this risk is further compounded by the lack of clear minimum or immutable standards that the system must comply with in order to ensure the preservation and protection of personal information, instead leaving such standards to the whims of the State.

169. The 2nd Petitioner also challenges the provisions of section 9A(2)(i) of the impugned Act which provides for the correction of errors in the register by a person or by the system on its own initiative to ensure that the information is accurate, complete, up to date and not misleading. The basis for the challenge of this provision is that it has been poorly drafted. This is because it affords to 'any person' the right to apply for rectification of 'any errors' in the register. Mr. Kegoro averred that this right should be restricted to the owner of the said information.

170. With regard to the provision for the State to rectify *errors 'of its own motion'*, Mr. Kegoro averred that as a secondary recipient of information, the State cannot, of its own initiative, determine what is or is not accurate, complete, up to date and not misleading information. It was his averment that the right of the State to amend any personal information should be exercised only with the consent and after consultation with the primary owner of the said information.

171. Mr. Kegoro averred further that the provision should also specify the applicable standards and principles for amendment of information. He gave as an illustration standards defining the scope and nature of personal information required under the Act in order to make it possible to anticipate with reasonable certainty whether an amendment is necessary.

172. The third reason advanced by the 2nd Petitioner for challenging the impugned Act relates to the process of its enactment. Mr. Kegoro averred that the impugned Act was enacted in a manner that denied the public the right to participate, a violation of Article 10(2)(a) of the Constitution. He stated that under Article 10(2) (a) and 118 (1) (b) of the Constitution as read together with Standing Order No. 127(3) of the National Assembly – 4th Edition, the National Assembly is enjoined in mandatory terms to facilitate public participation and involvement in the legislative and other business of Parliament and its committees. It is also enjoined to take into account the views and recommendations of the public made pursuant to such public participation.

173. It was his averment that to the best of his knowledge and the publicly available information, neither the public nor the 2nd Petitioner was given a reasonable or meaningful opportunity to comment on or contribute to the impugned amendments at any stage of the legislative process prior to their passage by the National Assembly. He deposed that given the nature, scope and effect of the impugned amendments, there is a real threat that as drafted, they will have far reaching, unintended and undesirable consequences on the enjoyment of all fundamental rights and freedoms under the Bill of Rights.

174. He averred that in the circumstances, it was imperative that concerns of members of the public arising from the amendments should be taken into account before the impugned amendments are operationalised. He noted in particular that the impugned amendments significantly alter the process and substantive right of identification and registration of persons from birth to death, including the right to acquire vital documents like birth registration certificates, student registration for enrolment and issuance of examination
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 30 of 205.

certificates, national identity cards, refugee cards, work permits, passports, driving licenses and death certificates. In his view, permitting the amendments to stand without public participation or contribution shall render the provisions of the Constitution and the Parliamentary Standing Orders that require public participation academic.

175. Mr. Kegoro deposed that from his position as the 2nd Petitioner's Executive Director in which he interacts with many members of the public from diverse backgrounds, he is aware that there exist grave concerns regarding the impugned amendments which would have been substantially addressed through the relevant committees of the National Assembly had the public been accorded the opportunity prescribed by law.

176. The 2nd Petitioner's second concern relating to the process of enactment of the impugned Act relates to the propriety of the procedure adopted. Mr. Kegoro averred that it is a universally settled precept that substantive amendments with far reaching consequences such as the impugned amendments should be effected through a substantive Act and not through a miscellaneous amendment in an omnibus Act. It was his averment that this position has been expressed by the courts and even by members of the National Assembly during debates in the house on similar Bills, including in the debates recorded in the Hansard of 20th November 2018 on the impugned Act. He contended that given the substantive and controversial nature of the impugned amendments, it was inappropriate and contrary to public interest that the amendments were enacted into law through an omnibus Statute Law (Miscellaneous Amendments) Act.

177. Mr. Kegoro averred that the concern with respect to the manner of amendment was brought to the attention of the National Assembly on 28th August 2018 through a point of order raised by Hon. Otiende Amollo but was ignored. He sets out in his affidavit the portions of the Hansard in which the Hon. Member's concerns were captured.

178. He asserted that using an omnibus Bill for a substantive subject such as is covered by the impugned Act is tragic given that there have been ongoing legislative efforts since 2012 aimed at achieving the same objectives as the impugned amendments, but through substantive Acts of Parliament. He cited the National Registration Identification Bill 2012 and the Registration and Identification of Persons Bill, 2014 (Senate Bill No. 39) which concerned the same issue as the impugned amendments. It was his averment that all these efforts have been short-circuited by an omnibus Miscellaneous Amendment Act. He observed that the two Bills contained safeguards relative to the impugned amendments in the impugned Act. He specifically pointed to the Kenya Citizens and Foreign National Management Service Act No. 12 of 2012 as containing similar functionalities as the impugned amendments but with better in-built safeguards. In his opinion, the impugned amendments were passed through an omnibus Bill in order to avoid strict scrutiny that they would otherwise undergo in stand-alone substantive Acts of Parliament.

179. The final ground of challenge to the Act set out in the affidavit of Mr. Kegoro is that the Act is ambiguous and lacks specificity, which he terms a violation of Article 94 of the Constitution as well as international law standards and practice. According to Mr. Kegoro, Article 94 (6) of the Constitution decrees that every Act of Parliament that confers on any State organ, State officer or person the authority to make provisions having the force of law in Kenya shall expressly specify the purpose and objectives for which that authority is conferred, the limits of the authority, the nature and scope of the law that may be made, and the principles and standards applicable to the law made under the authority.

180. He averred that the impugned amendments in this case are mired in generalities and ambiguities; that they essentially grant the relevant Cabinet and Principal Secretaries extensive powers to gather personal information and to make regulations with regard thereto without substantive framework limitations as to what information gathered may be used for or the principles and standards that should be applied in the exercise of the said powers.

181. Further, that the amendments introduce a weaker yet similar system as was established under the Kenya Citizens and Foreign National's Management Service Act No. 12 of 2012. He averred that as both laws are in operation on the same issue, without transitional provisions or interoperability modalities, there is currently confusion and ambiguity that may be exploited at the expense of the people. The net effect of this confusion is that the personal information of citizens is exposed to serious risk of abuse without accountability.

182. Mr. Kegoro averred that the danger to personal data that he expounds upon above is compounded by the lack of a policy and legal framework for privacy and data protection in Kenya, which implies that the State will have a *carte blanche* as to what and how to utilize personal information for. According to Mr. Kegoro, the impugned amendments are susceptible to abuse and fall far short of the UN Principles on Personal Data Protection and Privacy, the African Union Convention on Cyber Security and Personal Data Protection as well as comparable laws from other jurisdictions on limitations to the right to privacy.

183. He averred that if indeed the only purpose of the impugned amendments is to harmonise registration and identification of persons for efficient service delivery by the State, the flaws in the legislation render them unreasonable relative to their intended purpose.

184. It was Mr. Kegoro's contention that given the nature and scope of the rights in question, operationalising the impugned amendments will effectively amount to a repeal of substantive fundamental rights protected under the Bill of Rights, thereby exposing citizens to whimsical and unreasonable intrusions into their privacy by the State without their consent.

185. The 2nd Petitioner takes the position that the impugned law is unconstitutional for failure to involve the Senate in its enactment. Mr. Kegoro deposed to this effect in his Further and Supplementary Affidavit sworn on 12th April 2019. He placed reliance on Article 96 as read with Article 110 of the Constitution which he stated provides that any law that affects the functions and powers of county governments set out in the Fourth Schedule ought to be approved and passed by the Senate. He averred that in light of the admission by the Respondents that NIIMS will be used for statistics and planning, which is clearly a shared role between the national and county governments, the impugned law was accordingly unconstitutional as it was not approved by the Senate.

186. Mr. Kegoro further averred that the impugned amendments seek to register children as well as adults. This was clearly contrary to the Act which, at section 2, limited the application of the Act to citizens of Kenya who have attained the age of eighteen years or are of the apparent age of eighteen years or over. He contended that as the restriction in this section had not been amended by the impugned Act, its application to children, refugees and all other non-citizens or persons whose citizenship is undetermined, including stateless persons and persons at risk of statelessness, is illegal or *ultra vires*. He observed that the Director of the National Registration Bureau had, in his replying affidavit sworn on 21st February 2019 clearly stated that the national registration authority has a mandate to collect and keep a register of Kenyan citizens above the age of 18 only.

187. In any event, according to Mr. Kegoro, the form currently being used by the Respondents to collect data has no basis in law as it has clearly been developed without the legislative oversight required under the Interpretations and General Provisions Act Cap 2 of Laws of Kenya.

188. Responding to the claim by Ms. Janet Mucheru in her affidavit sworn on 26th February 2019 on behalf of the 2nd and 3rd Respondents that NIIMS seeks to protect children from trafficking, Mr. Kegoro suggested that this was not likely to be the outcome. He averred that in the course of its work with stateless communities like the Shona who are predominantly children of descendants from Zimbabwe, the 2nd Petitioner had established that Shona children, despite being registered within six months from birth as required by the Registration of Births and Deaths Act, are not issued with birth certificates.

189. Mr. Kegoro noted that according to organisations like United Nations Children Emergency Fund (UNICEF) and the International Labor Organization (ILO), undocumented children, children of migrants and stateless children are generally marginalised and at a very high risk of statelessness. It was his view that as structured under the Act, NIIMS applies strictly to adults and cannot offer protection from trafficking to undocumented and stateless children as averred by Ms. Mucheru.

190. In his view, the impugned amendments have not addressed the underlying structural issues facing stateless and other undocumented persons. It would therefore merely entrench and exacerbate the problems that these groups face in the digital sphere. He contended that the fact that the NIIMS system is entrenched in a law that does not apply to stateless persons, refugees and aliens is a clear indication that the impugned amendments had the intent to continue marginalising stateless persons rather than recognizing and granting them valid legal identity.

191. Mr. Kegoro averred that any legal regime for identification of persons in the digital age should, according to the World Bank, comply with the **Principles on Identification For Sustainable Development: Toward the Digital Age**. Such principles include ensuring universal coverage for individuals from birth to death, free from discrimination; removing barriers to access and usage and disparities in the availability of information and technology; and establishing a robust, unique, secure, and accurate identity.

192. It was his averment that the impugned amendments have placed emphasis on data collection and retrieval with limited or no regulation of critical facets of data protection relating to data minimization, collection, purpose limitation, and retention limitation that are the backbone of an effective data and privacy protection legislation. A worse failing of the amendments, in his view, was that not a single standard had been prescribed by the impugned amendments and none acknowledged for the purpose. It was his averment that this lacuna falls far short of the guaranteed standard of the right to privacy and comparative standards in data privacy and registration laws in jurisdictions that have proposed similar laws for collection of personal information.

193. Mr. Kegoro averred that the impugned amendments, held against the standards set out in UNESCO's International Declaration on Human Genetic Data, the AU Convention on Cyber Security and Personal Data Protection (Chapter II thereof), the European Union's General Data Protection Regulations (GDPR) and comparable national legislation from other jurisdictions, had been purposefully designed to collect personal information without safeguards for protections and mitigation of attendant risks. He reiterated the general motif of Petition 56, 58 & 59 of 2019 (Consolidated) | Page 33 of 205.

the 2nd Petitioner's grievance against the impugned legislation that it makes wide and ambiguous provisions for collection of personal data but does not provide substantive law for the protection of data retrieval, processing, storage, use and disclosure.

194. Mr. Kegoro gave several illustrations with respect to the lacuna in the law. He noted, first, that by their generality, the amendments compel data collection from everyone without regard to the unique differences inherent in a modern society; and that the impugned law does not anticipate the special circumstances that may call for special regulations in the collection of data from, adults, children, persons with disability or convicted criminals, among others. It was his averment that no effort had been made, with regard to children, to defer to their special interests and vulnerabilities as minors. He contrasted this with the European Union's GDPR which recognizes children's vulnerability and the additional support measures necessary to keep them safe in the digital age and accordingly makes specific provisions intended to offer them additional protection in the evolving data age.

195. The second failing identified in the impugned law by the 2nd Petitioner was what was perceived as the opaqueness that surrounds the actual software that has been deployed for NIIMS. Mr. Kegoro averred that the nature, capabilities, ownership details and other critical features of the system were known only to the State, with no information with regard thereto known by the public. He discounted the 5th Respondent's assertions that it designed and developed NIIMS with the combined effort of an inter-ministerial taskforce specifically formed for this purpose as a bare statement. In his view, there is no way of verifying that NIIMS meets minimum integrity, transparency and accountability standards as would guarantee privacy of personal information stored therein from unintended third parties or from abuse from within.

196. According to Mr. Kegoro, measured against the ideal legislative framework for a secure, transparent and verifiable system, the NIIMS system fell short, as it was impossible for example, to answer questions such as where the personal data gathered is being stored, for how long the data will be held, whether there are automatic notification mechanisms whenever data stored and processed in the system is accessed, and to whom the State can disclose the data. In contrast with the opacity in NIIMS, Mr. Kegoro cited the GDPR which he averred dedicates considerable provisions to guidelines for the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In his view, judging from the State's admissions, the system appeared to have been developed well before the enactment of the impugned laws, which gave credence to the fear that the system was arbitrarily developed and its security and integrity safeguards, if any, fall far short of international standards for similar systems.

197. The third weakness identified by the 2nd Petitioner related to the collection of DNA under the NIIMS system. Mr. Kegoro averred that in light of the capabilities of DNA highlighted in the affidavit of Mr. Davies Malombe, its collection without specific, restrictive and mandatory safeguards on how it may be used threatens every aspect of the citizen's privacy. He reiterated the apprehension expressed on behalf of the 2nd Petitioner by Ms. Munyua and Mr. Malombe that through the unhindered access to people's DNA, the State will be able to profile and share individuals' religious, political, cultural, health, criminal and other pre-dispositions without their consent.

198. In his response to the grounds of opposition filed by the 6th Respondent, Mr. Kegoro denied that there had been inordinate delay in filing the Petitions. He noted that the impugned
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 34 of 205.

Act was assented to on 31st December 2018, and commenced operations on 18th January 2019, while the Petition was filed barely 30 days from the said date. In any event, according to Mr. Kegoro, jurisprudence in this country since the advent of the 2010 Constitution had established that the doctrine of laches did not apply in cases for the enforcement of the Bill for Rights.

199. With respect to the 6th Respondent's claim that there had been public participation in the enactment of the impugned amendments, Mr. Kegoro averred that such claims consisted of bare allegations and fell far short of the standard of proof of public participation, the burden in respect of which fell on the Respondent. The said burden has not been discharged, and there was no evidence that Parliament took any measures to facilitate meaningful participation or to involve the public in the law-making process beyond the newspaper publication that merely listed the names of the Acts to be amended in the omnibus Bill.

200. Mr. Kegoro made similar averments with respect to the grounds of opposition filed by the 1st Respondent. He observed that aside from consisting of bare denials, there was no attempt by the 1st Respondent to respond to the substantive issues raised in the Petition. He asserted that in any event, as established by judicial precedent, Parliament and the State bear the burden of proving, to the requisite standard, that public participation in legislative processes had been facilitated.

201. In his response to the replying affidavit sworn by Dr. Karanja Kibicho on 26th February 2019, Mr. Kegoro averred that, as pleaded in the Petition, the 2nd Petitioner was not opposed to the establishment of NIIMS. Its opposition was only to the extent that NIIMS had failed to provide sufficient safeguards for fundamental rights and to prevent abuse. Mr. Kegoro averred that the justification for a modern registration system is not disputed. What the 2nd Petitioner was concerned with was that such a system should be alive to the equally advanced and sophisticated threats and capabilities for abuse that, unless checked by force of law, expose the people to serious threats of violation of inalienable fundamental rights and freedoms.

202. In his view, the NIIMS did not have clear, verifiable, accountable and secure checks and counterchecks to safeguard individual rights of privacy and security of the person as the Data Protection Bill 2018 that prescribe these safeguards had not yet been passed into law. He contended that whereas digitisation of certain public service systems may improve service delivery, extra precautionary measures must be taken to guard against increased threats of 'single point of entry type' breaches by internal and external parties to the detriment of the public, and without data protection laws, these threats intensify.

203. Mr. Kegoro reiterated that whereas the purpose of NIIMS may have been well envisioned, its implementation under the prevailing circumstances is a serious threat to the right to privacy, a fact which the affidavits of Alice Munyua from the Mozilla Group and Dr. Fisher from Privacy International had attested to.

204. Mr. Kegoro noted that the **Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis on Existing Identification and Registration Systems in Kenya** analysis report filed in court by the Respondents recommended the adoption of an effective law that would, among other things, ensure the security of any data collection system in light of the increasing threats of breaches and theft of vital citizen records in the digital age.

205. Mr. Kegoro averred that the fact that, as deposed by Dr. Kibicho, personal information collected under the impugned Act will be in the exclusive custody of the government presents

opportunities for abuse. It was his deposition that comparative best practices and standards for data protection recommend, among other things, the creation of an independent data protection authority to oversee the State as the processor and controller of protected information and thereby enhance accountability and protection from abuse. It was his view that NIIMS as established is essentially a self-policing data controller, processor and protection authority.

206. Mr. Kegoro reiterated the argument by the 2nd Petitioner that the amendments had not met the constitutional threshold for public participation. He based this contention on three grounds. First, that the call for submission of memoranda in respect of the Statute Law Miscellaneous Amendment Bill No. 12/2018 merely lists the Registration of Persons Act as one of the laws to be affected by the amendments. No further information was published as regards the content or impact of the proposed amendments in order to meaningfully facilitate informed public involvement in the law-making process. His second reason is that in the departmental committee reports, there is no record of any discussions of the substance of the amendments to the Registration of Persons Act, and in his view, in light of the inadequacies of public participation, this was not a coincidence. Finally, he contended that there is no record that the departmental committees received or considered any memorandum from the public in respect of the contentious amendments.

207. It was his averment therefore that there was no evidence that the Respondents complied with Articles 10 and 118(1)(b) of the Constitution. In his view, the purported public awareness efforts undertaken by the Respondents through newspaper articles and interviews were subjective one-sided efforts merely aimed at promoting the adoption of the system rather than facilitating meaningful or informed public involvement in the process.

208. With respect to the information required under NIIMS, Mr. Kegoro averred that the collection of individuals' DNA by force of law and for no specific purpose is intrusive and excessive relative to the purpose for which the NIIMS has been established. His contentions in this regard were in consonance with the averments of Mr. Davis Malombe, the Deputy Executive Director of the 2nd Petitioner, with regard to the collection of DNA, and the risks that such collection, storage and use of DNA posed to data subjects.

209. Mr. Davis Malombe in turn made detailed averments with respect to the ethics and legality of collection of DNA in his affidavit sworn on 12th April 2019. Mr. Malombe noted that as DNA pertains to entire populations, Kenya would be required to be compliant with international conventions and standards with respect to collection of DNA.

210. He expressed the opinion that the inclusion of DNA in the expanded scope of personal information that may be biometrically collected for purposes of registration of persons under the impugned law is excessive and unjustifiable. He averred that collecting DNA under the prevailing circumstances poses serious threats to protection of human dignity and privacy of the people of Kenya and sets out various reasons for taking this position.

211. Mr. Malombe relied on the International Declaration on Human Genetic Data, unanimously adopted by UNESCO in 2003, according to which DNA is essentially information about heritable characteristics of individuals obtained by analysis of nucleic acids or by other scientific analysis. DNA is extracted from a sample of a person's cells contained in, among other things, blood, hair roots and saliva which is analyzed in a laboratory to obtain the required genetic information, which can be stored as a string of numbers on a computer database.

212. He averred that the impugned law sanctions collection of DNA without the consent of the subject, and collection of DNA without consent is regarded as a violation of a person's bodily integrity. He contended that while a number of countries do sometimes collect DNA without consent from a limited number of citizens, this occurs only in circumstances prescribed by law, where such violations are regarded as necessary and proportionate to the need to investigate criminal or terrorist offences. However, in order to do this, extensive legal safeguards and tight restrictions on whose DNA may be collected in this way must be adopted.

213. Mr. Malombe further averred that DNA contains various parts which can be used for different purposes. He noted, by way of illustration, that the International Declaration on Human Genetic Data recognizes various DNA capabilities as including that they can be predictive of genetic predispositions concerning individuals; they may have a significant impact on the family, including offspring, extending over generations, and in some instances on the whole group to which the person concerned belongs; they may contain information the significance of which is not necessarily known at the time of the collection of the biological samples; they may have cultural significance for persons or groups, they may be used to track and identify individuals and their family members; and if further analyzed, DNA can reveal even more detailed information such as a person's health or other human capabilities that should otherwise remain private.

214. He contended that genetic information is therefore regarded as sensitive personal information and the declaration obligates member States to regulate the collection, processing, use and storage of DNA for specific limited and strictly regulated purposes such as diagnosis and health care, medical and scientific research.

215. Mr. Malombe took the position that the impugned amendments fly in the face of the above precautions by sanctioning unrestricted and mandatory collection and storage of DNA in digital form. He contended that the impugned Act makes no restrictions on what genetic information may be collected, what it may be used for, who it may be shared with and the basic standards that must be observed in the collection, processing, use, storage or disclosure of such information.

216. While conceding that DNA may be collected for forensic or criminal investigations, it was his view that even in these circumstances which have been established in a number of countries, whole genomes are not normally used and a legal restriction is normally put in place to restrict genetic information to specific parts of the genome referred to as 'non-coding' DNA. He contended that a forensic DNA profile is obtained and stored, based on only parts of the DNA, which do not reveal personal characteristics.

217. According to Mr. Malombe, this limits the interference with an individual's right to privacy by preventing personal information regarding health and other physical characteristics from being stored. Such forensic DNA profiles act as a 'genetic fingerprint' or biometric, enabling individuals to be identified through matching their stored DNA profile with a DNA profile from a crime scene, for example. However, unlike other biometrics, a forensic DNA profile can also be used to identify relatives (including paternity and non-paternity) and make inferences regarding the ethnicity or ancestry of the individual. He averred that forensic DNA profiles are therefore also regarded as sensitive personal information.

218. According to the 2nd Petitioner, indiscriminate collection of genetic information under the prevailing legal circumstances in Kenya make such information susceptible to extraneous

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 37 of 205.

use, including negative profiling of individuals for ulterior motives. Mr. Malombe observed that a person's DNA is left wherever they go, for example on a coffee cup, and this means a DNA database allows the government, police, or anyone who gains access to it to track individuals and their families, even if they have not committed crimes. This can be done by matching a DNA profile, found for example on a coffee cup at a political meeting, with a stored DNA profile in the computer database, which then provides details about the individual's name and address, among other things.

219. Mr. Malombe averred that if the whole population is on a DNA database, such database is open to abuse by governments or anyone who can infiltrate the system: for example by criminals wanting to track down victims, including high profile figures such as politicians or members of the security services, whose safety may be dependent on not revealing their identities.

220. A further reason advanced by the 2nd Petitioner against the collection and storage of DNA is that unlike fingerprints, DNA profiles can be used to identify an individual's relatives. This was so because an individual inherits half their DNA from their father and half from their mother, and a DNA database of a whole population can be used to find a person's parents, children, siblings and more distant relatives by comparing their DNA through a process of searching a DNA database known as "familial searching". According to Mr. Malombe, if a person's father or child is not really biologically related to them, "non-paternity" can be discovered easily by comparing the DNA profiles of the father and their supposed children.

221. Mr. Malombe contended that the discovery of non-paternity can have very serious impacts on families, and it was his averment that in most countries, relatedness and non-paternity is regarded as a private matter that may be investigated within the family but should not be exposed by others, including by the police or government. He argued therefore that building a universal DNA database risks the break-up of families by making it easy to discover non-paternity. He alleged, by way of illustration, that databases could be misused by a corrupt official or anyone who can infiltrate the system and gain access to the data, and if criminals gain access to information about non-paternity, they might blackmail an individual or their family by threatening to reveal this information.

222. Mr. Malombe averred further that an individuals' genetic information may also be analysed to identify more distant relatives or infer genetic ancestry or lineages. This, in his view, raises additional concerns that a DNA database may be used to facilitate identification of, and potential discrimination against, persons of different ancestries.

223. According to Mr. Malombe, there are currently no comprehensive international safeguards for DNA databases, which are also susceptible to errors and false matches. This risk increases when the database is expanded because more samples are being analyzed and more computer searches are being conducted. Mr. Malombe cited the most frequent source of errors in these circumstances as being the mix-ups or contamination of samples, either at the laboratory or before the samples get there. He further observed that errors are also more likely to occur where DNA from a crime scene contains a mixture of cells from more than one person, which he noted is often the case in rape cases. He further noted that a person's DNA can also be transferred to a murder victim or a weapon, even if they never touched it, falsely implicating them in a crime. He illustrated the challenges of mix-up in DNA by citing several

examples from media reports in England and the United States about persons who had been charged and in some cases convicted following mix-ups in DNA analysis.

224. Mr. Malombe averred that no other country in the world has legislation which allows the mandatory collection of DNA from whole populations, or inclusion of DNA as part of a national identification system. He averred that mandatory collection of DNA from whole populations violates international principles on human rights.

225. Mr. Malombe averred that to meet international privacy standards enshrined in the International Covenant on Civil and Political Rights and the Constitution, a DNA collection and retention mechanism must be extensively regulated, narrow in scope, and proportionate to meeting a legitimate security goal. Further, that international best practice would require Kenya to incorporate further safeguards into its DNA gathering system, including legal provisions to restrict the circumstances in which DNA may be collected and retained, and restrictions on the purposes for which stored data may be used. In his view, the impugned amendments fail this test.

226. Mr. Malombe cited a report titled **‘Establishing Best Practice for Forensic DNA Databases’** with respect to the key best practices for the protection of privacy in the collection of DNA. These include regulations on fully informed consent, quality assurance of laboratories, restriction of purposes, rules for expungement of data and destruction of samples. He averred that these safeguards should be enshrined in law before establishing a DNA database. Like the other deponents for the 2nd Petitioner, Mr. Malombe’s prayer was that the court should protect the rights of citizens and allow its Petition.

227. The third deponent who swore an affidavit in support of the 2nd Petitioner’s case was Ms. Alice Munyua, who described herself as the Policy Advisor, Africa, of the Mozilla Corporation, the maker of the Firefox browser used by hundreds of millions of people around the world. She averred that from her work with Mozilla, she had gained substantial expertise and competence on issues of privacy, security, data protection and digital ID, and had engaged with governments around the world on the said issues.

228. Ms. Munyua conceded that there is no doubt that legal identification is generally valuable for society, and that such legal identification schemes are enablers for the effective delivery of services and engagement between government and its citizens. She cited in this regard the UN Sustainable Development Goals (SDGs) which call for *"providing legal identity for all, including birth registration"* by 2030. She averred that without these commonly recognized forms of official identification, individuals are at risk of exclusion.

229. Ms. Munyua contended that at Mozilla, it had been recognised that Kenya appeared to have various challenges with the current legal identification system. She also observed that the Office of the Ombudsman in the Commission on Administrative Justice (CAJ) in Kenya had, in 2015, declared a crisis in the issuance of legal documentation in Kenya. That it had also provided evidence of widespread discrimination in access to documentation of identity, including access to proof of citizenship. In her view, transitioning to a digital identification system without first addressing the existing problem of widespread discrimination will not solve these problems. It will, rather, introduce several additional grave concerns including violations of privacy, security risks, increased discrimination and exclusion. Ms. Munyua relied in support on the CAJ investigation report on the crisis of acquiring identification documents in Kenya.

230. According to Ms. Munyua, transitioning to a digital biometric identification model is not required in order to realize the benefits of legal identification. She averred that to assume that "leapfrogging" to digital identification is inherently superior ignores the risks that digital, particularly biometric identifications, bring when deployed on a national scale.

231. Ms. Munyua averred that the digital features and infrastructure of digital identification projects have very different implications from their analogue legal identification initiatives. She contended that, contrary to the assertions by the Respondents, the addition of biometrics like iris scans, ear lobe geometry and DNA data is a dramatic expansion of the existing legal identification system which goes beyond mere digitization. It was her averment that biometric and DNA linked digital identification creates profound threats of invasive privacy violations, and the potential for misuse is very high. In her view, the linking of databases has the potential to turn the NIIMS system into a pervasive means of identification, tracking, and control, as well as increase the risk of large-scale data breaches, concerns that were serious enough to require that the government allows sufficient discussion, examination and scrutiny through public consultations.

232. Ms. Munyua contended that NIIMS, like other similar national biometric identification systems, was a centralised database of the most intimate details of a country's residents. That through the legislation authorising NIIMS, the government was contemplating collecting a wide range of extremely sensitive information, including DNA, iris scans, earlobe geometry, and fingerprints. It was not clear, according to Ms. Munyua, what purpose collecting all of this highly sensitive information serves and whether the means proposed in the law are the minimum necessary to accomplish this purpose.

233. She averred that it was increasingly universally recognized that data collected is data at risk; that 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. It was her deposition that while it is tempting to use biometrics as an easy way of ensuring the uniqueness of enrollees to a system, such use increases the risk associated with an identification system. In her view, if and when a biometric database is breached, DNA and fingerprints cannot simply be reset like a password, and it was also far from clear that biometrics are the only way to ensure uniqueness and avoid duplicative enrolment.

234. Ms. Munyua averred that a breach of an identification database is not just a theoretical harm. To illustrate, she cited the situation in India where, despite the government's claims that the Aadhaar database was '100% secure', there have been repeated reports of the demographic data being compromised, which has made it difficult to trust the resilience of the system against malicious practices. Citing an online article, she observed that a private citizen in India had been able to buy access to all of the demographic data in the Aadhaar database for just 500 rupees (Kshs 727). She further observed that other online reports indicated that it was possible to purchase editing rights to the Aadhaar demographic database for a mere 2,000 rupees (Kshs 2909).

235. In further illustration of the risks of digital identifications, Ms. Munyua gave the example of Estonia whose system, which had allowed cryptographic keys to be generated on a smartcard rather than a general-purpose computer, had been praised for its security and sophistication.. She averred that the system had, however, become vulnerable when the cryptographic library was compromised, necessitating significant measures to mitigate the risk. It was her contention that 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 of breaches. In her view, it was unclear whether Kenya has the resources or infrastructure to mitigate a similar breach of NIIMS.

236. In supporting the position taken by the Petitioners that Kenya should have used ‘open source’ in the design of NIIMS, Ms. Munyua deposed that her company embraces ‘open source’. She stated that the term referred to “*something people can modify and share because its design is publicly accessible.*” She further averred that “*the open source way*” and “*open source projects, products, or initiatives embrace and celebrate principles of open exchange, collaborative participation, rapid prototyping, transparency, meritocracy, and community-oriented development.*” She argued that as a company embracing open source, Mozilla has found significant benefits in open sourcing all of its codes, including for products like Firefox, as this allows many individuals, including security researchers around the world, to find and report vulnerabilities in its codes. Ms. Munyua argued therefore that 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 enrolment and send or share information.

237. Ms. Munyua made further averments in her affidavit regarding the dangers of a centralized database like NIIMS with extensive sensitive biometric data. It was her testimony that 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. In her view, breach of systems like NIIMS were not a remote risk, and it was a safe operating assumption that the database will be compromised, and she cited by way of illustration the breach of India’s Aadhaar system.

238. While conceding that seamless transfer of information between government departments may be desirable for governance, Ms. Munyua contended that there are better alternatives to achieve this without breaching privacy rights. She supported this contention by referring to the Estonian system in which the databases of each department and service provider are held separately and are connected through the X-Road data exchange layer that manages the exchange of information as needed by each programme.

239. Ms. Munyua expressed the view that an identification database that is primarily meant for welfare delivery should not be misused for law enforcement or intelligence surveillance. She averred that NIIMS may create a transaction log of all authentication requests linked to specific identification numbers. According to Ms. Munyua, 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.

240. Ms. Munyua contended that in order to mitigate the risk of misuse for law enforcement or intelligence surveillance, 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. She cited in this regard a paper by **Edgar Whitley** titled ‘**Trusted Digital Identity Provision: GOV.UK Verify’s Federated Approach**’.

241. Ms. Munyua further made various averments regarding the shortcomings in the process of establishing NIIMS. She cited in particular the lack of public participation in the process, noting that under the 2010 Constitution, public participation is now a constitutional right and an obligation on the part of the government. It was her averment that NIIMS was authorised
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 41 of 205.

through changes made to the Registration of Persons Act through the Statute Law (Miscellaneous Amendments) Act and was not subjected to public participation. She further argued that the amendments to the Act came into force on January 18, 2019, only 19 days after the President gave his assent, without public consultation or parliamentary debate.

242. Ms. Munyua averred that there was insufficient protection for data provided for NIIMS. She contended that while the government asserts that there is a data protection policy and bill that informed the development of NIIMS, the Bill is still pending debate in Parliament. It was her view that no digital identification system should be implemented without strong privacy and data protection legislation; that 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.

243. Ms. Munyua contended that individuals should always be in control of their digital identities and biometrics, and it was particularly egregious that NIIMS was passed even as a strong data protection law is under consideration by the Kenyan Parliament. In her view, the proposed Data Protection Bill of 2018 is a strong and thorough framework which contains provisions relating to data minimization, collection, purpose and retention and if it was in effect, NIIMS would likely be in conflict with its provisions.

244. According to Ms. Munyua, the data protection law should establish an empowered, independent regulator to ensure that rigorous regulations and standards are set on how to handle personal data processing. It was also her view that an independent data protection authority is critical to ensure the data protection law is enforced.

245. It was also Ms. Munyua's averment that the main features and processes of the identification system, especially those affecting the rights of users, must be enshrined in the primary law. She contended that 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. In her view, an independent regulator can help to protect the rights of Kenya's residents, but those rights must first be established in law.

246. With respect to the security of the system, Ms. Munyua took the view that the position taken by the respondents that the system was secure because section 20 of the **Computer Misuse and Cyber Crimes Act, 2018** provides enhanced penalties for offences involving protected computer systems does not make the NIIMS system secure. It was her averment that making an attack of a system a crime does not actually make it secure. Her opinion was that legal penalties alone have never served as a sufficient deterrent against malicious actors. She cited in this regard the situation in India where, despite the legal prohibitions against publishing Aadhaar numbers and breaching the system, there have been multiple public leaks and breaches, including by state governments, citing the case of the State of Andhra Pradesh which had allegedly build India's first police state using data from Aadhaar.

247. Ms. Munyua further contended that relying aggressively on laws that criminalize accessing a computer system without authorization had another downside in that it can disincentivize and threaten security researchers. She averred that security researchers play a critical role in finding and reporting vulnerabilities in a system so that they can be patched in an expeditious manner. She argued that some of the most effective security research involves probing computer systems without the explicit permission of the owner of that system. Her position, as we understand it, is that governments should not criminalise accessing computer

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 42 of 205.

systems as this would deter security researchers, thus leaving the systems vulnerable and making the identity system and the deeply private information stored in it less secure.

248. Ms. Munyua argued further that the NIIMS process should not be used for exclusion. She observed that 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 a *Huduma Namba*, the potential consequences of being excluded from enrolment in the system were immense. It was, consequently, important that no one is excluded from the identification system because of their physical, social, demographic, or economic characteristics. She noted in particular the potential exclusion of marginalized communities through the process of enrolment into the system as officials will be using existing documents to prove and verify who is a citizen, thus locking out people who do not have these documents. She averred that the gap of conclusive proof of citizenship already affects many Kenyan communities, including the Makonde, the Shona as well as pastoral communities and tribes.

249. It was her averment further that those who are already enrolled in the system might also be at risk of exclusion due to the features of NIIMS that might end up enabling discrimination. She observed that collection of DNA data can be used to identify an individual's ethnic identity, and given Kenya's history of politicization of ethnic identity, collecting this data in a centralized database like NIIMS, which can be linked to other databases, could reproduce and exacerbate patterns of discrimination. Reliance for this averment was placed on a report from the 2nd Petitioner titled **'Politicization of Ethnic Identity in Kenya: Historical Evolution, Major Manifestations and the Enduring Implications'**.

250. She further noted that in India, the requirement of the Aadhaar ID number for access to HIV medication was feared to increase the risk of stigmatization and further discrimination, citing a report in which it was noted that HIV positive people had dropped out of treatment programmes as treatment centres insisted on Aadhaar registration. It was her averment that for such vulnerable communities, the possibility of a record being maintained and potentially shared in unauthorized ways was an unacceptable risk.

251. With regard to the question of best practices on digital identification systems, Ms. Munyua criticised the examples of best practices cited by the 5th Respondent, notably United Kingdom, Estonia, India, and Malaysia. She contended that the projects in these countries have been highly criticized or are not relevant comparisons. With regard to the Estonian model, it was her averment that it is a federated system and is in stark contrast to the integrated model put forth by the government of Kenya. As for the Malaysian and Indian models, her averment was that serious concerns have been raised with regard to privacy, data protection, governance, and cyber security as well as concerns related to system design and the inclusion or exclusion of people from government and some private services. In relation to the United Kingdom DNA database, it was her averment that it was not an identification system at all. It was, rather, a forensic DNA database maintained by the United Kingdom police for those implicated in crimes and was governed by strict data retention norms which require that the records of individuals found innocent be deleted. Her averment was that this system was in stark contrast to NIIMS which would take the DNA data of the entire population, rather than merely those suspected or convicted of crimes.

252. Ms. Munyua asserted that the United Kingdom's government's identification system, *Verify*, does not include biometrics and has a completely federated identification architecture which has been commended for its decentralized approach that gives users control. It was also her averment that the United Kingdom was not an appropriate comparison since, like most of the other countries mentioned by the Respondents, it has had strong data protection law and enforcement in place since 1984.

253. She noted that while the Respondents had taken the position that India's Aadhaar identification project has been heralded as a success story, they had ignored much of the criticism that has plagued the project. She averred that with the demographic data in Aadhaar reportedly compromised, it was hard to see how the system can be trusted for authentication. According to Ms. Munyua, a more worrying aspect of Aadhaar was that hundreds of thousands of people have been denied access to basic services, including access to food, because they either do not have an Aadhaar (digital identity) card, or their digital identity is "incomplete" because their fingerprints have not been uploaded to the national database due to poor internet connectivity.

254. Expert evidence was presented for the 2nd Petitioner by Ms. Grace Bomu Mutung'u through her witness affidavit sworn on 12th April 2019. She was also cross-examined at the instance of the 2nd and 3rd Respondents.

255. Ms. Mutung'u described herself as an Advocate of the High Court of Kenya and a researcher and specialist in digital rights and internet governance. She stated that she had over 10 years' experience in internet governance digital rights work and held advanced certifications on information controls from Harvard University. Her witness affidavit was sworn in support of the 2nd Petitioner's petition, and particularly in addition to paragraph 10(a), (corrected at the hearing to paragraph 14(a)) of the further and supplementary affidavit of Mr. George Kegoro sworn on 12th April 2019.

256. Ms. Mutung'u averred that Kenya is a signatory to international conventions that call for the protection of the privacy of children. She cited Article 10 of the African Charter on the Rights and Welfare of the Child which guarantees to all children the right to privacy; the Convention on the Rights of the Child which also protects a child's right to privacy at Article 16; as well as Article 40 with respect to legal proceedings.

257. Ms. Mutung'u averred that universal principles on digital privacy laws acknowledge that processing of children's data requires additional protection. She cited the European Union's General Data Protection Regulations (GDPR), recital 38, which provides that children merit specific protection with respect to their personal data as they may be less aware of the risks, consequences and safeguards and their rights with respect to their personal data.

258. She averred that the principles require special consideration of children when processing their data. She noted that when considering fairness and lawfulness, attention should be given to the fact that children are still in their formation and are therefore likely to change as they mature to adulthood. Consequently, digitalization of their lives should be done in a manner that does not prejudice their future opportunities.

259. She noted, by way of illustration, that while digital systems may be used to capture children's educational journeys, caution should be applied when capturing subjective aspects. Thus, the system should be designed to take in factual aspects such as the name, parentage and schools the child attended. It should, however, avoid opinions such as reasons for a

child's good or bad performance in school. Should it be necessary to record such opinions, they should be removed from decision making technology, and automated decisions should never be made on the basis of subjective opinions.

260. Ms. Mutung'u cited the United Kingdom Data protection regulator, the Information Commissioner's Office (ICO)'s recommendations to data controllers processing children's data. It recommends that they consider the basis for processing of children's data and design systems and processes that respond to children's specific needs. Among the principles she cited include consent to the processing of the data, though she avers that this may not be adequate protection of privacy, particularly with respect to children because of the power asymmetry between the data processor and the subject. She noted that in many instances, users of online services need the service and consent is presented as a step one has to accept by clicking on in order to proceed to the service, a challenge that is more profound for children who may not have the full capacity to understand information presented to them.

261. The second principle she cited relates to the purpose for which the data is required. Ms. Mutung'u averred that since children's data can be used to profile them in prejudicial ways, the purpose for which the data is collected must be very clearly stated.

262. Ms. Mutung'u further noted the need to observe the principle of adequacy in the collection of data relating to children. Her averment was that the nature of big data systems requires collection of as much data as possible for big data analytics, which abrogates the right to informational privacy where one's data should not be unnecessarily required. It was her averment that children are in an especially vulnerable position in relation to big data as they are ever growing, their biological features are maturing with significant changes, and big data systems would require their data to be constantly updated, leading to constant surveillance. It would therefore be necessary, in her view, in order to ensure safeguards on adequacy, to determine why children's data is being collected in the first place, a function that would best be covered in laws or regulations.

263. A fourth necessary principle with regard to children's data, according to Ms. Mutung'u, is accuracy, the need for data processors and controllers to ensure that children's data is accurate. To achieve this, parents or guardians should be given an opportunity to view the children's data and to correct and update it as may be necessary.

264. According to Ms. Mutung'u, a data system should also take into consideration the principle of retention in relation to children's data, given the transitory nature of childhood and the increased capacity that comes with it. She averred that children's data, which is collected and processed without their full awareness, should therefore not be stored eternally. Upon reaching adulthood or the age of consent, children should be able to make decisions on their data, including moving with it to other systems or having it completely destroyed.

265. Concomitant with this right is the right of children as data subjects. While they may have no capacity to make decisions involving their data, like other data subjects, they can exercise these rights with the assistance of an adult such as a parent or guardian. Ms. Mutung'u averred that regulations should define how children may achieve their data subject rights and the role of parents and guardians in this regard.

266. Ms. Mutung'u further averred that there should be clear provision with respect to data security. She observed that in a country like Kenya where children form a significant part of the population, their data is of great interest to the government but also to data analytics who

would want to study the collective traits of Kenyans. She averred that children's data is therefore highly valuable and requires high protection at all times.

267. Finally, Ms. Mutung'u averred that there was a need to ensure that there was no cross-border transfer of children's data, and that there should be assurance that children's data shall not be transferred to jurisdictions without adequate data protection.

268. It was her averment that no attempt had been made in the impugned law to provide for the above safeguards. In her view, the inescapable conclusion was that the said law gives the State unfettered power to gather children's data without concomitant responsibility to protect children against possible threats of abuse or derogation of their privacy.

269. In cross-examination by Mr. Regeru Ms. Mutung'u confirmed that she had not presented any documents to the court regarding her expertise on children's digital rights. She had sworn her affidavit in support of paragraph 14(a) of George Kegoro's affidavit, which she conceded had been responded to by the affidavit of Karanja Kibicho (for the 2nd and 3rd Respondents) sworn on 14th May 2019. She maintained that no system exists in respect to children's digital data or with respect to the digital data of stateless persons and refugees.

270. Ms. Mutung'u maintained that while Kenya was a signatory to the Convention on the Rights of the Child and the African Charter on the Rights of the Child and had made commitments with respect to the rights of children, looking at the amendments to the Registration of Persons Act, Kenya had made no attempt to protect children's digital data. She conceded, however, that there is no published information on NIMS and her averments were based on the amendments to the Registration of Persons Act.

271. Ms. Mutung'u also conceded that from the affidavits sworn on behalf of the 5th Respondent by Loyford Muriithi, she had noted mention of encryption, which gives protection to children and adults. She had also noted his averment that as regards children's identity data, additional or special technical safeguards were incorporated in the architectural design of NIIMS database with a view to providing the requisite safety. She did not know how NIIMS affects the rights of children as she was not familiar with the architecture and functioning of NIIMS.

272. Ms. Mutung'u stated that none of the legislation in force, including the Children Act and the Counter-trafficking Act, offer protection to children, and neither did the amendments to the Act align it to the Constitution. In her view, children's data is not being used to trace children, though it may lead to their tracing.

273. Taken through the averments by the Respondents on the benefits of NIIMS, in particular that digital national master population registers are crucial in enforcing rights nominally enshrined in law by providing greater legal protection, and that NIIMS could help in the elimination of trafficking in children, child labour, as well as help enforce laws against child marriage, she asserted that in her view, there was no benefit to NIIMS given the manner in which it was designed; that digitisation of children's data was a harmful cultural practice and harmful choices were being made for children; and that once they were digitised, they could not 'undigitalize' themselves. As she saw it, the problem with NIIMS was the centralisation of data.

274. With regard to the data capture form for the *Huduma Namba*, her view was that it did not have provision for consent of parents, just confirmation that one has given their data to government.

275. In cross-examination by Dr. Nyaundi, Ms. Mutung'u maintained that there should be more safeguards and the system should have been discussed before data collection for children started. In her view, if there are safeguards in place, it would be in order to collect children's data. She asserted that there should be purpose limitation and clarity on why children's data was being collected, as well as limitation on who can access that data once it has been collected, as well as being very clear on what happens to the children as regards their data when they attain the age of majority. She disputed the suggestion that biometric registration will reduce cases of child labour and child trafficking.

276. In response to questions from Mr. Bitta, Ms. Mutung'u maintained that the law relating to data collection contained in the Act is deficient in certain respects, and to the extent of the deficiency, the law is unconstitutional. She confirmed that under Article 1 of the Constitution, the people of Kenya have given power to the legislature to legislate, but the court had power to question a law or policy on the basis that it is not efficacious, and can ask the legislature to correct the legislation. She conceded that the technical aspects of a legislation would be found in subsidiary legislation, not the main Act, and that the information being sought under NIIMS is necessary to the government for, among other thing, knowing where children are born, their residence and parentage.

277. In re-examination, Ms. Mutung'u stated that while it was necessary to know where children are born, among other things, it was not necessary to have such information in digital form. She expressed the view that the amendments to the Act had abrogated human rights and, in respect to children, there was no legal provision for collection of children's data or issuing identity cards to children. Ms. Mutung'u referred to section 2 of the Act to confirm her contention that the Act applies only to Kenyans who are above 18 years.

278. While agreeing with the views expressed in the affidavit of George Kegoro in support of the Petition and the need for special protections for children who are a vulnerable group, she took a critical view of NIIMS on the basis, first, that children's data was collected without a legal basis and secondly, there was no consideration of the question whether it was necessity to collect children's data and then digitise it or in other words change children into data. In her view, it was necessary, in the circumstances, to ask the questions set out in Article 24 of the Constitution, whether it was necessary to collect children's data, and whether there were less abrogating ways of collecting this data and safeguarding it and protecting the privacy and dignity of children.

279. With respect to the architecture and design of NIIMS, Ms. Mutung'u stated that the 2nd Petitioner had requested for information about the technical capability of NIIMS and how it was being developed from the Ministry of Interior in December 2018 but they had not received a response.

280. Ms. Mutung'u made reference to the averments by George Kegoro with respect to the collection of DNA, the immutability of DNA, and that once it is collected, it is permanently stored. She testified that should the database containing DNA be breached, it would threaten the privacy of every person. It was her contention further that the State will have unhindered access to people's DNA and be able to profile and share the individual's religious, political, cultural, health, criminal and other predispositions without their consent. With regard to children, the concern was that malevolent actors may want to profile children and manipulate their lives and behaviour.

281. To the question whether the digitisation of data would stop child trafficking, Ms. Mutung'u reiterated her response in cross-examination that it would not, noting that there were cases, such as in India, where children were registered by people other than their parents, and in her view, registration under NIIMS would not stop trafficking.

282. On the provisions of Article 24 of the Constitution, Ms. Mutung'u's evidence was that there was no legitimate basis for collecting children's identity data as section 2 of Act does not envisage collection of children's data or issuance of identity to children. In any event, in her view, there are less restrictive measures, or measures that would promote their rights more. There was nothing in the law in her view that would safeguard children, a vulnerable part of the population, as the law was silent on and does not address the issue of children in any way.

283. Ms. Mutung'u expressed the apprehension that everyone was being reduced to data and that only a person with a digital personality can receive services. Further, that the idea that one can only receive services if one has a digital personality was suggestive of the creation of a new legal regime or a new law of personality, a digital personality, on the basis of which one would receive services. This, in her view, goes to the core of the Constitution and the sovereignty of the people of Kenya, raising the question whether one was no longer a person in the eyes of government if one does not have digital personality. She further expressed the apprehension that NIIMS, which was touted as a single source of truth, could be taking the country back to centralization of power as the person who can view the data has a lot of power.

284. Ms. Mutung'u reiterated the views that she had expressed in her witness statement regarding the absence in the law of the principles that are a requisite for data protection in relation to the special nature of children and therefore provide special protection for children when processing their data. She maintained that the law does not provide for the principle of fairness and lawfulness, and no consent was sought or any explanation given to children or their guardians with regard to the purpose for the collection of their data.

285. Ms. Mutung'u asserted that no explanation was given on whether there were no less invasive means of achieving the same purposes sought to be achieved with the impugned law, without putting the lives of children at risk. She testified that the principle of adequacy, which requires that only what is sufficient for the intended purposes is collected, was not adhered to. It was her contention that we are now living in an age where data is the new oil, and there is a push to collect as much data as possible on people. In her view, however, the principles of data protection, especially the principle of adequacy, requires that only such data as is sufficient for the intended purpose, which purpose should be stated beforehand, should be required. Considering that children are still in their formation, if the government starts collecting data on them now and keeps collecting more and more data and profiling them, a lot of decisions on the lives of children will be made based on this data. It was therefore necessary to collect only what is sufficient for the stated purposes.

286. As regards the principle of accuracy, it was Ms. Mutung'u's testimony that from the design of NIIMS, there is absolutely no opportunity for children or their caregivers to view what data the government has on them and to correct what is incorrect. Yet, such data is used to make decisions, including legal decisions, that affect their lives. With respect to the principle of retention which Ms. Mutung'u testified is related to the principle of adequacy, her view was that data should not be kept in perpetuity but only for the period when it was

required. These issues, in her view, were not addressed in the impugned amendments, and it was not known how long the data was going to be stored, the possibility being that it would be kept eternally.

287. As for the rights of data subjects, it was her testimony that these should have been captured in regulations; that the Act should have been made in a way that would have allowed for regulations that would define how children may achieve their right to access, correct, and update the data, and the manner of transiting with the data upon reaching adulthood, to decide what should be done with the data collected prior to adulthood.

288. With regard to security of children's data, Ms. Mutung'u testified that it was not known how secure the data was. Further, that there is no publication that states what measures have been put in place to secure the data, and in the event of a breach, that there are good systems to mitigate any harm that may arise from the breach. On the issue of cross-border transfer of data, Ms. Mutung'u testified that the Petitioners just needed an assurance that children's data will not be exported to be used to train artificial intelligence systems; and that if it is exported, it will be used in jurisdictions that have adequate data protection laws.

289. In countering suggestions from the Respondents that she did not have the expertise that she claimed in children's digital rights, Ms. Mutung'u explained in re-examination that she had studied information technology at Strathmore College specialising in management of information systems. She had studied law at the University of Nairobi and had interned under Professor Ben Sihanya, a Professor of IT and intellectual property. She had studied Internet Governance at the University of Malta, and thereafter was awarded a fellowship in 2016-2017, renewed in 2017-2018, at the Berkman Klein Center for Internet and Security housed at Harvard Law School. She had participated in and given input on all the Bills that have to do with information, communication and technology, including the Access to Information Bill (now the Access to Information Act) and the Data Protection Bill then pending before Parliament.

The 3rd Petitioner's Case

290. Kenya National Commission on Human Rights (KNCHR) is an independent human rights institution created by Article 59 of the Constitution, and established by the Kenya National Commission on Human Rights Act of 2011. Its mandate is to protect and promote human rights in Kenya, and to uphold and defend the provisions of the Bill of Rights. It filed a petition dated 18th February 2019, which is supported by the affidavit and further affidavit of Dr. Bernard Mogesa sworn on 18th February 2019 and 21st May 2019 respectively.

291. The 3rd Petitioner echoed the concerns raised by the 1st and 2nd Petitioners with respect to the process of enactment and substance of the impugned amendments. It specifically cited the lack of public participation, the use of the omnibus Bill and violation of the right to privacy. The 3rd Petitioner raised an additional ground that the impugned amendments violate the constitutional right to dignity by making the collection of DNA mandatory, contending that DNA collection is invasive and should only be taken for specified and well recognized reasons.

292. The 3rd Petitioner prays for:

- a) A declaration that the amendments introduced to the Registration of Persons Act through the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018 are unconstitutional null and void .***

b) A declaration that the amendments introduced to the Registration of Persons Act through the Statue Law Miscellaneous (Amendment) Act No. 18 of 2018 are unconstitutional, null and void for being in violation of Article 10 and 118 as read with Article 259 of the Constitution.

c) A declaration that the amendments introduced to the Registration of Persons Act through the Statue Law (Miscellaneous Amendment) Act No. 18 of 2018 are unconstitutional, null and void for infringing on the right to privacy and the right to public participation.

d) An order prohibiting the Respondents, by themselves, their employees, agents and/or servants from installing the National Integrated Information Management System in any manner howsoever until effective policy, legal and institutional frameworks are put in place.

e) An order prohibiting the Respondents, by themselves, their employees, agents and/or servants from implementing the National Integrated Information Management System in any manner howsoever, until effective policy, legal and institutional frameworks are put in place.

f) A declaration that the entire legislative process introducing substantive amendments through a Miscellaneous Act was flawed and defective and is thus null and void.

g) Being a public interest suit, no orders as to costs do issue.

The 3rd Petitioner's Evidence

293. In his affidavit in support of the Petition and his further affidavit, Dr. Brian Mogesa averred that the impugned amendments violate, among others, Article 31 of the Constitution on the right to privacy, and Articles 10 and 118 on the national values of governance and public participation. He averred that the amendments were enacted unprocedurally by way of an omnibus Bill which is not appropriate for such major and extensive amendments. It was also his contention that the Bill should have been referred to the Senate for approval before enactment.

294. Dr. Mogesa further deponed that the impugned amendments have introduced a broad definition of biometrics that differs significantly from that provided in the Data Protection Bill. Additionally, he contended that the amendments will enable the government to obtain from individuals Global Positioning Systems (GPS) co-ordinates. It was his contention that these amendments will lead to inordinate and arbitrary storage of needless and intrusive confidential information in violation of Article 31 of the Constitution.

295. According to Dr. Mogesa, there are no policy guidelines regulating the management and security of the data. It was his deposition therefore that the implementation of the impugned amendments would subject individuals to grave risk of unauthorized disclosure of confidential personal information, including their location.

296. In his further affidavit, Dr. Mogesa responded to the averments by the 6th Respondent on the issue of public participation by averring that the constitutional principle of public participation presupposes that the public ought to have been engaged in a meaningful and qualitative manner. It was his contention that the said standard was not met. In his view, the advertisement of the amendment Bill in the newspapers by the Respondents was a cosmetic

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 50 of 205.

attempt to give the illusion that the public had been accorded an opportunity to participate in its enactment.

297. According to Dr. Mogesa, the Respondents had resorted to threats to counter the opposition to the impugned amendments, and he annexed copies of newspaper excerpts of statements made by government officials to the effect that certain services would not be availed to those without a *Huduma Namba*, and that there would be no extension of the registration period for the said number.

298. The 3rd Petitioner conceded that it sent a memorandum to the National Assembly on the impugned amendments. It was Dr. Mogesa's averment, however, that the original Bill that the 3rd Petitioner sent a memorandum on was later substantially changed. He asserted that in any event, the mere fact that the 3rd Petitioner gave its views to Parliament does not mean that these views constituted sufficient or meaningful participation by the public. He annexed a copy of the 3rd Petitioner's Memorandum on the Statute Law Miscellaneous (Amendments) Bill of 2018 dated 25th May 2018.

299. It was Dr. Mogesa's averment, however, that the 3rd Petitioner is not against the introduction of NIIMS. Its only concern was that the introduction of NIIMS was not in compliance with the Constitution, and there was no clear legislative framework for protection of the data collected.

THE CASES OF THE INTERESTED PARTIES SUPPORTING THE CONSOLIDATED PETITIONS

300. The Interested Parties who supported the Petitions were Muslims for Human Rights, Haki Centre, Law Society of Kenya, and Inform Action, which filed affidavits in support of the Consolidated Petitions. The 3rd Interested Party, Muslim for Human Rights (Muhuri) is a non-profit organization that works on promoting and advancing human and people's rights for communities in all regions of Kenya. It filed a Replying Affidavit sworn on 24th April, 2019 by Khelef Khalifa, the Chairman of its Board of Directors.

301. On its part, the 4th Interested Party, Haki Centre, is a non-governmental organization that promotes the progressive realization of human rights and active participation in addressing the issues of citizenship and statelessness. It also filed a Replying Affidavit sworn on 8th April 2019 by Phelix Lore, its Executive Director.

302. The 5th Interested Party, Law Society of Kenya, is a statutory corporate body established by section 3 of the Law Society Act, Cap 18 of the Laws of Kenya, and one of its objectives is to assist the government and courts on legislative matters and the administration and practice of law in Kenya. It filed a Replying Affidavit sworn on 14th March, 2019 by its Chief Executive Officer, Mercy Wambua.

303. The last Interested Party who supported the Petition was the 6th Interested Party, Inform Action Limited, which is a human rights organization that empowers communities. It filed a statement dated 8th April, 2019.

304. The Interested Parties' averments are substantially to the same effect as the averments made by the Petitioners on both the procedural and substantive infirmities of the impugned amendments, as well as the shortcomings of NIIMS.

305. The particular areas underscored by the Interested Parties were the lack of information and public participation in NIIMS; its threat to the right to privacy and insufficient data

protection provisions; the use of an omnibus Bill to enact the impugned amendments and lack of Senate's participation; the perpetuation of marginalization and exclusion of vulnerable groups who face challenges in getting registration as Kenyans; and the lack of limitations on the powers to be exercised by the public officers in charge of NIIMS.

306. The 3rd and 6th Interested Parties in addition contended that the impugned amendments seek to limit the enjoyment of fundamental rights and freedoms, but do not meet the threshold for such limitation set out in Article 24 of the Constitution, to the extent that they do not specify and address the parameters set out in that Article. They contended, in particular, that the new data sought to be collected under NIIMS has no rational connection with the stated objectives of the Act, nor are they reasonable and justifiable in an open and democratic society.

307. On its part, the 4th Interested Party in addition put forward a case for stateless persons. It contended that just like Nubians, stateless persons are unable to access documentation of citizenship in Kenya, which has resulted in restrictions in enjoyment of rights and freedoms guaranteed under the Bill of Rights and under international and regional human rights instruments. Further, that stateless persons are limited in access to birth registrations, identity documents, education, healthcare, employment, property ownership, political participation and freedom of movement which are enshrined in the Constitution. It was its case that stateless persons will be further discriminated against by NIIMS if adequate safeguards are not put in place by the government.

308. The 5th Interested Party, elaborated on the discriminatory practices and profiling that are likely to be caused by NIIMS. It contended that vulnerable groups such as children and the elderly who, for lack of identity documents or poor quality of fingerprints, may be locked out of the system, will not be able to get services. Further, that persons may also be targeted from the data collected by NIIMS for personal, commercial and political gain.

309. The 5th Interested Party further contended that under NIIMS, it is possible for the government to control the economic, social and cultural existence of individuals, and to control access to subsidized food supply, healthcare, and social welfare among other important social services, which undermines the sovereignty of the people of Kenya.

THE RESPONDENTS' CASES

The 1st Respondent's Case

310. The 1st Respondent is the Honourable Attorney General who is the principal legal adviser to the government of the Republic of Kenya and represents the national government in court. His office, powers and responsibilities are as established under Article 156 of the Constitution of Kenya and the Office of the Attorney General Act No. 49 of 2012. The 1st Respondent filed grounds of opposition dated 20th February 2019 and 26th February 2019 in response to the Consolidated Petitions. It was his contention that the Petitions do not disclose any threat of violation of the Constitution; that the Petitions are premised on conjecture and misconceptions that negate the substance and object of NIIMS; and that the formulation and enactment of the impugned amendments were made within the confines of a proper and justified legislative process. He contended further that the registration of persons is a process regulated by the Births and Deaths Registration Act and the Registration of Persons Act and the NIIMS process is primarily anchored on the said legislation.

311. As regards the allegation by the 1st Petitioner that the Nubians have faced discrimination in the registration process, his response was that the allegation lacked a factual and legal basis. In his view, to have the State accord the Nubians preferential treatment over and above other Kenyan citizens is contrary to the provisions of Article 27 of the Constitution.

312. The 1st Respondent further took the position that NIIMS seeks to capture and store data in a centralized digital database for effective and efficient administration which will facilitate accountability in various forms and curb wastage of resources in line with Article 201 of the Constitution. It would also ease registration and identification of persons thereby improving the security of the country by authenticating and verifying persons. Moreover, by attempting to direct the manner in which the impugned legislation ought to have been enacted, the Petitioners were asking the court to question the legislative wisdom of the National Assembly contrary to Chapter Eight of the Constitution yet they had failed to demonstrate that the parliamentary procedure was flouted in the process leading to the enactment of the impugned amendments. It was the 1st Respondent's contention therefore that the Petitioners had failed to discharge the evidentiary burden required of them to prove non-compliance with Article 118(1)(b) of the Constitution as read with National Assembly Standing Order No. 123 as regards public participation in the process leading to the enactment of the impugned laws.

313. According to the 1st Respondent, public participation can in any event be effected directly by the people or indirectly through their democratically elected representatives in the National Assembly which courts have taken judicial notice of. Furthermore, the Petitioners had failed to explore the option provided under Article 119(1) of the Constitution as read with the provisions of the Petition to Parliament (Procedure) Act No. 22 of 2012 before seeking redress from this Court. It was his contention further that the Petitioners have failed to rebut the presumption of constitutionality that is enjoyed by the impugned amendments.

314. The 1st Respondent conceded that data protection is crucial. He argued that contrary to the Petitioners' claim that there are no data protection laws, data in Kenya had been secured under various statutes including section 83 of the Kenya Information and Communication Act and section 20 of the Computer Misuse and Cyber Crimes Act.

315. It was also his contention that the right to privacy is not an absolute right. Further, that the Petitioners have not demonstrated how the limitation to the right to privacy fails to meet the dictates of Article 24 of the Constitution, if at all, and they had also failed to outline the vagueness in the impugned law or the opaqueness in the manner in which it is being implemented.

316. To the contention that the impugned amendments were unconstitutional for not receiving Senate approval, the Attorney General asserted that under the Fourth Schedule to the Constitution, national security, immigration and citizenship, national statistics and data on population are functions of the national government. Consequently, there was no requirement to involve the Senate during the enactment of the impugned law.

317. Regarding the use of an omnibus Bill to enact the amendments, the 1st Respondent stated that the impugned amendments are not substantive and therefore their enactment through a Statute Law (Miscellaneous Amendment) Act was justified.

The 2nd and 3rd Respondents' Case

318. The 2nd Respondent is the Cabinet Secretary in the Ministry of Interior and Co-ordination of National Government, while the 3rd Respondent is the Principal Secretary in the Petition 56, 58 & 59 of 2019 (Consolidated) | Page 53 of 205.

said Ministry. The two Respondents are public offices established by the Constitution as part of the Executive branch of Government and are responsible for *inter-alia* the registration of persons services under the Registration of Persons Act.

319. In response to the Petitions, the 2nd and 3rd Respondents filed three Replying Affidavits all sworn by Dr. (Eng). Karanja Kibicho, CBS, on 26th February 2019. They also filed a Further Affidavit sworn by the same deponent on 14th of May 2019. The 2nd and 3rd Respondents also filed a further affidavit sworn by Janet Mucheru on 26th February, 2019.

320. Dr. Kibicho deposed that he is one of the three Principal Secretaries in the Ministry of Interior & Co-ordination of National Government. He is also, pursuant to section 9A(3) of the Registration of Persons Act (as amended by Statute Law (Miscellaneous Amendments) Act No. 18 of 2018), the administrator of NIIMS. It was his averment that the government of Kenya has a responsibility to provide services to the people of Kenya and in order to fulfil its legal and constitutional responsibility, it requires adequate planning which in turn requires reliable data regarding its citizens and other persons within the country.

321. He deposed that collection of data and making it easily accessible for utilization by the government and other relevant stakeholders is therefore of paramount importance. It was his deposition that the government has been collecting relevant data from its citizens through multiple registration systems at different phases of an individual's life from birth to death by disparate agencies, thereby leading to duplication of efforts and wastage of resources. He averred that some of the government agencies would collect information from individuals but without any unique identifiers such as fingerprints thereby risking the accuracy and reliability of such information.

322. Dr. Kibicho stated that the existence of multiple population registration systems undertaken by disparate agencies under independent legislations resulted in a number of challenges. He identified these challenges as including duplication of efforts; wastage of public resources; incomplete population data; inefficient coordination and linkage of registration agencies; cases of identity fraud; and limited capacity to share information due to the manual storage of information.

323. He deposed that in light of the above challenges, the government, in 1989, conceptualised the development of one national population register as a single source of truth on the identity of individual citizens and foreign nationals residing in Kenya. It was his averment that although there has been some progress, this objective has not been met, and currently, approximately ten institutions which were collecting information from Kenyans in 1989 still do so and maintain mostly segmented and parallel databases. Dr. Kibicho stated that the NIIMS system was the culmination of the vision for a single national population register.

324. Dr. Kibicho narrated the events and steps that preceded the introduction of NIIMS since the initial concept in 1989. One of the key components of the initial idea was the creation of a National Population Register (NPR). In the year 2000, a concept paper was developed by the Office of the President for what would then become the Integrated Population Registration System (IPRS). In 2001, the concept paper was approved by the Cabinet which gave the go-ahead to the Office of the President and the Ministry of Finance to start the project. In 2002, the Office of the President initiated the development of its Information Communication Technology (ICT) Policy Framework and Strategic Implementation Plan for the years 2002-2005 which plan initially prioritized the creation of an ICT infrastructure linking all departments within it. In September, 2005, an Inter-Ministerial Taskforce on Integration of

Population Register Systems (IPRS) was appointed to fast track the integration of the registration systems. In its February 2006 concept paper, the Taskforce recommended, among other things, the introduction of a unique national number – Personal Identity Number (PIN) for all individuals resident in the country, assigned at birth, to serve as the control number for all registration systems.

325. It further recommended the establishment of a National Population Register, containing information of all residents, to serve as a central reference for all population registration systems. Further, that a central database be established to facilitate operations of the National Population Register. Finally, that a nationwide ICT infrastructure backbone be developed to link government agencies for purpose of information sharing and verification. These recommendations formed the basis for the subsequent operationalization of IPRS. It was his averment that the IPRS was conceived to provide a Common Reference Model (CRM) geared towards facilitating efficient coordination, linkages of registration systems, and information. Its purpose was also to enable convenient, equitable and innovative access by users to integrated government registration services under the larger scheme of e-government projects including the Integrated Financial Management System (IFMIS) among others.

326. According to Dr. Kibicho, some of the objectives of the IPRS were to develop a centralized national population register that would contain information of all Kenyans and foreigners resident in Kenya; to improve data storage and access in all population registration agencies; to facilitate efficient coordination and linkages of registration agencies; and to improve overall registration capacity within the registration agencies.

327. Nevertheless, IPRS had its own challenges which included the fact that an individual's data was still being collected by multiple government agencies, which resulted in continued wastage and inefficiency; that in some cases, the data being integrated into IPRS contained inaccuracies, pointing to the need to collect personal information from the source again; that information relating to children was not being captured comprehensively at birth; that IPRS did not constitute a master register which could be regarded as “a single source of truth” as it relied on information from multiple, sometimes conflicting, sources; and that the multiple registrations systems resulted in issuance of several identity documents such as identity cards, passports, driving licences and National Hospital Insurance Fund (NHIF) cards.

328. Dr. Kibicho averred that the above challenges were pointed out in a report prepared by the Ministry of Information, Communication and Technology and the United Nations International Children's Emergency Fund (UNICEF) after a Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis on Existing Identification and Registration Systems in Kenya. To build on the progress made by IPRS and address the challenges identified by the SWOT Report, the government initiated the NIIMS programme which was operationalised by Executive Order No. 1 of 2018.

329. The purpose of the NIIMS programme, according to Dr. Kibicho, was to create and manage a central master population database which will be the “single source of truth” on a person's identity and will serve as the only reference point for personal information for Ministries, Departments and Agencies (MDAs) and other stakeholders. His averment was that the main objectives of NIIMS are to collate, store, integrate, harmonize and facilitate sharing of population data from nearly all databases; provide a single source of truth (one-stop-shop) on persons' identity data for citizens and foreign nationals residing in Kenya; and to

undertake national biometric registration of all citizens and foreign nationals residing in Kenya.

330. It was his averment further that NIIMS is crucial for development planning and decision making. That it is also a key component of the government's service delivery commitments, currently prioritized under the "the Big 4 Agenda" which include food security, affordable housing, manufacturing and affordable healthcare.

331. Dr. Kibicho further highlighted some of the key benefits of NIIMS as including optimal utilization of scarce public resources; an accurate, reliable and comprehensive population registration database; verification, validation and authentication of primary data source; accurate population data for planning and service delivery; digital and inter-linked access to information for decision-making; and standardization and streamlining of relevant government processes.

332. Other benefits of NIIMS identified by Dr. Kibicho were access to registration services by all Kenyans; improvement of provision of security by government to citizens particularly in light of threat of terrorist attacks; improvement in enforcement of law and order including facilitation of early detection of fraudulent activities, minimisation of cases of identity theft and reduction of fraud in land transactions; to foster confidence and assurance in financial transactions due to the overall verifiability of personal information; and enhancement of tax collection.

333. Dr. Kibicho contended that by implementing NIIMS, the government is joining the global trend of adopting technology in service delivery. Further, that the implementation is in actualization of Kenya's commitment to the African Union regarding digitization, harmonization and integration of systems to promote efficiency in service delivery. The 2nd and 3rd Respondents contended that the government has spent a lot of money, time and other resources in actualizing NIIMS. It was their case that the government had successfully completed the pilot phase and intended to roll out the mass registration in the month of March 2019.

334. Dr. Kibicho denied that the government intended to collect DNA and GPS coordinates from citizens as alleged by the Petitioners. He averred that the data collection form had no provision for collection of DNA and GPS information, and that in any event, Kenya does not currently have the capacity to collect DNA information from all Kenyans. As regards GPS, it was his averment that the government's intention is to know the place of residence of each Kenyan. However, it does not intend to keep surveillance on their movements as alleged by the Petitioners. In his view, NIIMS is intended to protect individuals' rights to privacy by ensuring that all their personal identification information is secured in the custody of one government entity.

335. It was also his averment that Kenya has a robust series of statutes and policy on data protection, information security, modalities of access to information and protection of privacy of the integrity of government records and information. In his view, NIIMS has not introduced major changes to the information to be obtained from Kenyans. Instead, it has sought to update the government's method of collection and storage of information to take advantage of current technology for efficiency purposes.

336. Dr. Kibicho stated that the impugned amendments were subjected to meaningful and qualitative public participation in line with Article 118(1)(b) of the Constitution and had met

the threshold thereunder. He detailed the enactment process of the impugned amendments to buttress his averment and contended that members of the public and requisite stakeholders were given sufficient notice and adequate opportunity to participate in the consideration of the issues in the Bill. It was also his contention that members of the National Assembly, being the duly elected representatives of the people of Kenya, effectively represented the citizenry in the consideration and passage of the amendments. He had also personally sensitized members of the public on NIIMS through various public fora and media in his official capacity.

337. Dr. Kibicho averred that the impugned amendments were not substantive in nature as the personal information required for registration under NIIMS is essentially similar to the personal information required for registration under the registration systems which were already in existence before the amendments.

338. Regarding the failure to submit the Bill to the Senate, Dr. Kibicho deposed that the matters covered by the impugned amendments relate to national population registration, which is not a devolved function and is squarely within the mandate of the National Government. To the Petitioners averments that there were other Bills pending in Parliament on the same issue as the impugned amendments, Dr. Kibicho responded that the intended purposes of the National Registration and Identification Bill, 2012 and the Registration and Identification of Persons Bill, 2014 which have in any event since stalled in Parliament, are effectively achieved by the impugned amendments.

339. In response to the concerns raised by the Petitioners with respect to the procurement of NIIMS, Dr. Kibicho stated that the procurement of the hardware components of the NIIMS registration kits was conducted in strict compliance with the Constitution and procurement laws. Further, that owing to the sensitivity of NIIMS, its software component was developed internally by several government agencies under the stewardship of the Ministry of Information Communication and Technology and no foreign entity was involved, or will have access to the information collected by NIIMS.

340. The Petitioners contention that NIIMS will entrench discriminatory practices was denied. Dr. Kibicho averred that on the contrary, NIIMS will ensure universal coverage for individuals from birth to death, thereby eliminating any perceived discrimination against any individual or class of persons under the current disparate registration systems. He averred further, that in any event, the need for vetting of applicants for the issuance of legal identification documents upon attaining the majority age, as is currently the practice, would be unnecessary as the requisite personal information would already be in the NIIMS system. According to Dr. Kibicho, the complaint about the alleged discrimination under the current registration system being carried over to NIIMS has no basis. He noted that the Petitioners had not demonstrated what feature of NIIMS would make registration of alleged marginalized communities more difficult. He also dismissed the allegation of discrimination, noting that the 1st Petitioner had, in a letter dated 8th April 2017, paid glowing tributes to the 2nd, 3rd and 4th Respondents for a commendable job done in the registration of persons especially in areas where members of the 1st Petitioner reside.

341. Dr. Kibicho also observed that unlike the national identity card which is only issued at the age of majority, the registration for NIIMS will start as early as immediately after birth, thus easing access to services and exercise of constitutional rights. Vetting, if any, is in respect of issuance of national identity cards and registration for NIIMS does not require any vetting.

342. On the concerns raised by the Petitioners with regard to the registration of children, Dr. Kibicho averred that NIIMS will not hinder any child from enjoyment of the rights of a child, but will instead facilitate the enjoyment of such rights including the right to education, health, identity, nationality, and protection from child trafficking and protection from child labour.

343. In his affidavit sworn on 14th May 2019, Dr. Kibicho, averred, first, that no material evidence had been provided by Ms. Fatuma Abdulrahman to support the averments made under the heading “*Historical Review of Nubian Experience*” in her affidavit of 12th April 2019. It was his averment that the alleged discrimination against the Nubian community relates to shortcomings in the current registration system as opposed to NIIMS, which he contended will address any shortcomings.

344. According to Dr. Kibicho, NIIMS is not designed to, and will not discriminate against Nubians or any other ethnic community. He conceded that members of all border communities, which he defined as communities whose members are found within and outside Kenya, are subjected to vetting in order to ensure that only genuine citizens are issued with identification documents. It was also his position that vetting is further necessitated by national security concerns arising from security risks posed by porous borders. Vetting was therefore not discriminatory, but in any event, the vetting committees complained of were not introduced by the impugned amendments.

345. In response to a complaint by the 1st Petitioner that vetting for purposes of issuance of identity documents was done only twice a week, he averred that there is no regulation or policy stipulating that vetting is to be conducted only on Tuesdays and Thursdays of every week. It was his averment that vetting can be done on a daily basis depending on the number of persons desiring to acquire identity cards. He further stated that contrary to Ms. Abdurahman’s averments, the law requires a person to be issued with an ID card within 30 days of the application for those turning 18 and 15 days for replacement of a lost or unserviceable identity card. It was his contention that whenever an applicant appears before the vetting committee and is positively identified as a Kenyan, he or she is registered immediately thereafter. Dr. Kibicho clarified that that NIIMS registration process is meant to be a continuous exercise and all Kenyans will have an opportunity to register in the system.

346. As regards the decisions of the African Commission on Human and Peoples’ Rights and the African Committee of Experts on the Rights and Welfare of the Child, Dr. Kibicho observed that the decisions do not relate to NIIMS and are largely irrelevant to the gravamen of the present dispute. Further, that the said decisions were determined *ex parte*, and are in any event not binding on the Kenyan State. Dr. Kibicho noted that the 1st Petitioner had alleged that there were no local remedies available for determining the dispute relating to alleged discrimination, and in his view, it was an abuse of process for it to now seek to introduce it before this court.

347. Dr. Kibicho also addressed himself to the contentions by George Kegoro in his Further and Supplementary Affidavit sworn on 12th April 2019 that the National Registration Bureau has no authority to collect or store biometric data from children, stateless persons, refugees and foreigners; that NIIMS does not protect children from trafficking; that the form used to collect data has no basis in law; and that the personal information collected under the impugned amendments will be in the exclusive custody of the government rather than an independent data protection authority which opens opportunities for abuse. His response was that the rights of children, stateless persons, refugees and aliens are substantially protected

under the Constitution and existing legislation, including the Kenya Citizenship and Immigration Act, 2012, the Children's Act, 2001, and the Refugee Act, 2006, and that the impugned amendments do not in any way repeal these pre-existing legislation. Moreover, that the impugned amendments categorically provide for the registration of children on NIIMS. In addition, that registration onto NIIMS is not based on any form of discrimination on any ground including nationality, because it fully incorporates the registration of citizens and non-citizens currently residing in Kenya.

348. According to Dr. Kibicho, NIIMS registration is fully under the administrative supervision of the relevant Principal Secretary, and this effectively creates an extra level of supervision and accountability to ensure the overall effectiveness and integrity of the system. Further, that the form encompassing the data capture tool implements the text and spirit of the impugned amendments and is therefore formulated within the law.

349. Dr. Kibicho denied the contention by Mr. Kegoro that the impugned amendments do not comply with the legal principles that apply to digital identification of persons set out by the World Bank in the publication "**Principles on Identification for Sustainable Development: Toward the Digital Age.**" He averred that contrary to the averments by Mr. Kegoro that there is a lacuna in the impugned amendments as regards the retrieval, processing, storage, use and disclosure of the collected data and that there is a need for the establishment of clear legal safeguards to ensure accountability, NIIMS clearly encompasses the said Principles. It was his position that the 2nd Petitioner has not demonstrated how NIIMS has failed to meet any of the Principles, but that in any event, the said Principles are not binding on Kenya. In Dr. Kibicho's view, there already exists a healthy and robust legislative framework on data retrieval, processing, storage, use and disclosure of information such as is contained under NIIMS.

350. Response was also made to the averments by Mr. Kegoro that the collection of DNA without safeguards threatens the right to privacy and is intrusive; that despite the benefits of NIIMS and digitization in service delivery, precautionary measures must be taken to guard against breaches by internal and external parties; and that the constitutional objective of public participation was not met in NIIMS. Dr. Kibicho reiterated that NIIMS registration did not involve collection of DNA. He clarified however, that DNA collection is crucial in certain circumstances, such as prevention of crime including terrorism, and in the identification of bodies in case of accidents where all other biometrics are destroyed or unavailable.

351. It was his averment, however, that NIIMS will not be freely accessible by third parties, either private or foreign, and is predicated on the law, namely the Registration of Persons Act, which is operating within the larger legal framework on data protection. Furthermore, the government was in the process of enacting the Data Protection Bill, 2019 to bolster this framework. According to Dr. Kibicho, NIIMS as a single source of truth offers a more secure option of data protection by reducing the points for breaches, and as admitted by the 2nd Petitioner, this is the global trend in personal identification databases. He noted that despite the Petitioners concerns, over thirty-one (31) million individuals, representing approximately sixty-five percent (65%) of Kenya's population, were enrolled during the NIIMS registration exercise.

352. Pursuant to a notice to cross-examine issued by the Petitioners, Dr. Kibicho testified as DW3 and was cross-examined on his affidavit evidence set out above. He confirmed that the data capture form for the *Huduma Namba* registration had sections that required personal and

biometric bio-data. He further confirmed that although the form was primarily meant for personal identification, it also requested for other information on agricultural activities and employment status, a result of requests made by other Ministries who needed the said data and for whom data was collected in the same form for purposes of cost effectiveness.

353. Dr. Kibicho further confirmed that the statement in the form that indicated the registration was mandatory was later removed, and the only mandatory documents required for the registration were either an identity card, birth certificate, passport or alien card.

354. Dr. Kibicho acknowledged that some of the information sought in the data capture form was already held by various government institutions but averred that the information had become adulterated. The main purpose of NIIMS therefore is to confirm the correct information about a person accurately in digitized form to address this shortcoming. On the disclaimer in the data capture form, Dr. Kibicho explained that this was a form of consent that the information collected could be given to authorized government agencies.

355. Dr. Kibicho further explained that the government had tried to collate personal data through setting up the Integrated Population System. This, however, did not solve the problem of adulteration of the data. It was his testimony that the *Huduma Namba* process will provide an opportunity for verification of documents and cleaning up of the personal data held by matching and verifying it with documents held in other databases.

356. On the requirement for DNA in the impugned amendments, Dr. Kibicho testified that the purpose of including DNA was to provide for as many unique identifiers in the law as possible. There was, however, no intention to collect DNA even though it is permitted by law. He asserted that for the *Huduma Namba* registration, the only biometrics collected were digital fingerprints and digital photographs.

357. When questioned on the public participation on NIIMS, Dr. Kibicho testified that he and various government officials and the national government administration infrastructure had sensitized the members of the public and carried out civic education on the benefits of NIIMS. He denied that they stated or threatened that the registration for *Huduma Namba* was compulsory.

358. Dr. Kibicho was also cross-examined on the Data Protection Policy of 2019 and data protection principles of fairness, transparency, accountability and data minimization. He stated in response that the government was open to engagement on any issues that the Petitioners may have with NIIMS. His testimony was that the Registration of Persons Act was the legal framework for NIIMS, and for the purposes of the Data Protection Policy and Bill, the offices of Data Commissioner and Data Controller are yet to be established as the Bill is yet to be enacted.

359. It was his averment further that in relation to NIIMS, it is the Principal Registrar created in the Registration of Persons Act that is performing the functions of the Data Controller, and that the said Act also provides for offences if there is unlawful disclosure of data. He denied that the data collected on *Huduma Namba* will be exposed, maintaining that there are existing laws on data protection, and the Data Protection Bill is meant to consolidate these laws.

360. With regard to the application of the Registration of Persons Act to children, Dr. Kibicho disagreed that the Act does not apply to children under section 2 thereof. It was his position that it applies to all Kenyans including children, pursuant to the amendments made to the Act. He clarified that only birth certificates and not the fingerprints of children under the Petition 56, 58 & 59 of 2019 (Consolidated) | Page 60 of 205.

age of six (6) years were required during the *Huduma Namba* registration exercise. He also referred to the Executive Order that established the *Huduma Namba* Inter-ministerial Committee as providing the guiding laws on children.

361. With regard to the decisions of the African Committee of Experts on the Rights and Welfare of the Child on the discrimination against Nubian Children, Dr. Kibicho testified that it had been implemented by way of budgetary allocations for registration exercises. The government had also implemented Rapid Results Initiatives and affirmative action for Nubians and those who pass the vetting have been issued with identity cards. It was his testimony that the assertion by the Petitioners that Nubians are not given identity cards is a false one.

362. It was also his testimony that incremental registration of births of children was adopted under NIIMS, which is to be achieved by cleaning up of data on the births already registered and registering new births in the system. Further, that this approach arose from recommendations in the SWOT analysis undertaken by UNICEF and the benchmarking and study tours of the Estonian registration system.

363. Dr. Kibicho denied that the vetting of Nubians before issue of identity cards was done on ethnic grounds. He explained that the vetting is only done where a Registrar is in doubt about the citizenship of a person from the communities living in Counties bordering other countries, which he termed as border communities. With regard to the composition of the vetting committees, Dr. Kibicho clarified that the committees are identification committees set up under the Act and are government led, with local elders being included at the discretion of the Chair of the committee

364. He confirmed that those without identity cards were not registered with NIIMS but stated that the Respondents were making efforts to ensure that the Nubians are issued with identity cards, though he stated that it was not all Nubians who did not have identity cards. It was Mr. Kibicho's position that registration with NIIMS is a continuous process and one can be registered upon obtaining an identity card. Dr. Kibicho denied that NIIMS registration is necessary for service provision by the government but that it will be more convenient to get services with the *Huduma Namba*. In his view, it is for a person to choose if they wish to be inconvenienced or not.

365. With regard to whether a cost-benefit analysis of NIIMS had been done, Dr. Kibicho stated that taxpayers money of Kshs 7 billion had been spent so far on the system, and that at completion, Kshs 9 billion would have been spent. While the government was not asked to provide the costing on the benefits of NIIMS, such figures are available, and he had enumerated the benefits in his response to the Petitions.

366. According to Dr. Kibicho, the amendments to the Act were therefore minor as the new data collected was minimal, and it is the digitization of the data which is novel. He, however, conceded that there would be risks if the data is not protected. While protecting national security is one of the uses of NIIMS, the entire NIIMS data cannot be exempted from protection on grounds of national security, and that there are security laws which prescribe the circumstances when this can be done. He also confirmed that no rules were developed after the amendments of the Act to guide the *Huduma Namba* registration.

367. In re-examination by Mr. Regeru, Dr. Kibicho explained that digitization is one of the reform platforms of the government. While there had been other initiatives undertaken,

digitization of the population register was lacking and was needed to complement efficient service delivery. He reiterated his evidence on the public participation held, the mandatory documents that were needed for the *Huduma Namba* registration, that the said registration was not mandatory and that DNA was not collected nor is its collection planned during the exercise.

368. Dr. Kibicho explained that the physical attendance of a registrant is important in NIIMS for purposes of recording biometrics arising from the adulteration of existing databases, and the physical presence of a person is required to match him or her to the existing data. He also explained that people gave their consent by annexing a digital signature or thumbprint, and the incremental registration will result in a situation where everyone has only one unique identifier.

369. Dr. Kibicho stated that 31,500 *Huduma Namba* registration kits were acquired, and that they would be left with the Chiefs, Assistant Chiefs and civil registration clerks for continued registration. With respect to the question of vetting for identity cards, Dr. Kibicho reiterated that it is not unique to Nubians, it is done by Assistant Chiefs for all Kenyans, including among border communities, and the vetting committee is a second level of authentication where an Assistant Chief is not sure of a person's identity. He denied that border communities equate to tribe and clarified that everyone living at the border is part of a border community regardless of their tribe. He also denied that there has been discrimination against Nubians nor was there such government policy.

370. Dr. Kibicho pointed out that there is a website with information on NIIMS and that the administration and his ministry had given information on NIIMS, how it was to be rolled out, and its benefits. He enumerated the direct benefits of NIIMS including the savings made in collection of data and rolling out of services, the conduct of the population census and registration of voters. Further, that in the cost-benefit analysis, there are benefits of NIIMS that directly translate to money benefits while others are in the form of convenience in eternity as enumerated in his affidavit. Further, that the main costs of NIIMS was in the acquisition of the registration kits and payment of registration clerks.

371. According to Dr. Kibicho, the Data Protection Policy applies not only to NIIMS but to all data that is collected, and that the office of the Data Controller can only be appointed once the Data Protection Bill is enacted into law, and not on the strength of the policy. Dr. Kibicho testified that every institution that collects data from the public has a data administrator and laws that regulate the collection and management of the data, and the Bill is being enacted for efficiency reasons to tidy up existing laws.

372. Dr. Kibicho denied that there was a need for a *Huduma Namba* law before rolling out of *Huduma Namba* Registration. He maintained that the amendment to the Act was adequate as there were other existing laws as identified in the Executive Order on NIIMS implementation. He also clarified that under section 9A as read with section 2 of the Act, NIIMS applies to all Kenyans, including children, and that NIIMS had benefits for children in terms of planning for their health, education and other services. He further asserted that the government had submitted its report upon compliance with the recommendations made by the African Committee on the Welfare of the Child, and that the welfare of children is also a core principle in the Constitution.

373. Dr. Kibicho informed the Court that if allowed to process the data collected in NIIMS, all existing identity cards would be collapsed to one digital identity card- the third generation
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 62 of 205.

identity card- which will have an encrypted chip. Further, that each service provider would have a reader that only reads the information in the card that is relevant to it.

374. The second deponent on behalf of the 2nd and 3rd Respondent, Janet Mucheru deponed that she is the Director, Civil Registration Services, a department under the Ministry of Interior and Coordination of National Government. This department, is responsible for the registration of births and deaths that occur in Kenya and draws its mandate from the Births and Deaths Registration Act, Cap 149.

375. She detailed the functions of the Civil Registration Services and averred that it is mandated to register certain particulars which include the name, sex, date and place of birth, and the names, residence, occupations and nationality of the parents for any birth. As regards deaths, Ms. Mucheru listed the particulars registered as the name, age, sex, residence, occupation and nationality of the deceased, and the date, place and cause of death. She stated that the Cabinet Secretary in the Ministry has the discretionary power to prescribe any other particulars other than those set out in the Act, including biometric data.

376. It was therefore Ms. Mucheru's deposition that in registering births, the Civil Registration Services requests for substantially the same personal information as was being captured by the data capture form for NIIMS, and which information has always been in its custody and is therefore not new.

377. While making reference to the finding in the report by the Ministry of Information and Communication Technology in partnership with UNICEF titled **Strengths, Weaknesses, Opportunities and Threat Analysis of Existing Identification and Registration Systems in Kenya, December, 2017** that a birth certificate number is not unique, Ms. Mucheru set out the risks attendant with the manual collection and registration of birth particulars. She pointed out that there is a risk of duplication of records, loss of physical records, delays in processing birth records, ineffective service delivery when the need arises to share or verify the data on births with other agencies, and the lack of linkage between the birth and death of an individual.

378. Ms. Mucheru contended that the data processing, analysis and utilization by the Civil Registration Services can only be improved by the use of technology and deposed that the use of NIIMS will prevent cases of identity theft where certain individuals may use the identity of a dead person for criminal purposes. It was also her deposition that the said Report recommends that all citizens be electronically registered at birth to ensure accurate collection and storage of data that will become the "*single source of truth*." She further deposed that digitization of this data by NIIMS will ease service delivery by the Civil Registration Services by facilitating efficiency in the production and maintenance of the register of births and deaths. It was also her contention that the integration of personal information with biometrics through NIIMS will enhance the integrity of the records of births and deaths that are maintained by the Civil Registration Services.

379. With regard to children, Ms. Mucheru averred that NIIMS would facilitate enjoyment of the rights of children because the current registration systems do not uniquely identify children and have aided in the prevalence of child trafficking in Kenya as noted in the Trafficking in Persons Report, 2017. Further, that due to the fragmented nature of the registration systems, there have been cases of falsification of documents resulting in illicit adoptions where children have permanently been separated from their families. Due to the unreliable records on children and the resultant irregular adoptions, the government had

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 63 of 205.

issued an indefinite moratorium in inter-country and resident adoption and revoked licences to conduct inter-country adoptions to protect children in Kenya.

380. Ms. Mucheru enumerated the benefit of NIIMS to children. She averred that with NIIMS, the traceability of a child's parents prior to adoption is ensured. Further, that a reliable biometric identification will effectively ease the process of re-uniting children with their families when compared with the present process of reunification which is lengthy, tedious and costly as it requires publication in the newspapers or DNA testing of parents. In her view, with a DNA database, identifying the parent will be simplified by comparing a child's DNA to available DNA profiles.

381. It was her deposition further that the introduction of biometrics to the registration of births will enable the Civil Registration Services to ascertain the identity of a child and curb child identity theft by linking that child's biometric to a specific *Huduma Namba* as issued through NIIMS and eventually, to their parent (s). Further, that it will ensure children are not subject to various bureaucratic registration processes in different stages of their development. Ms. Mucheru asserted that reliable data on children will also ensure proper planning during emergency situations such as drought, famine or war and ensure provision of essential services to children during the period of separation.

382. Ms. Mucheru highlighted other benefits that will accrue to children as a result of registration in NIIMS, including, eliminating the need for verification of citizenship, enhancing public health as a result of more efficient immunization using a child's *Huduma Namba*, accessing education, enabling government to plan for the welfare of children, identifying children in conflict with the law, and detecting and remedying child labour and sexual exploitation. By digitizing the process therefore, the registration coverage of births and deaths will be raised by 100% by 2020 in line with the Civil Registration Service's strategic objectives.

The 4th and 7th Respondents' Case

383. The 4th Respondent is the Director of the National Registration Bureau, which is an office in the Ministry of Interior & Co-ordination of National Government. It is responsible for the implementation and enforcement of the Registration of Persons Act and, specifically, the identification, registration and issuance of identity cards to all persons who are citizens of Kenya and who have attained the age of eighteen years. The 7th Respondent is the Kenya Law Reform Commission, established by the Kenya Law Reform Commission Act No. 19 of 2013 with the mandate of reviewing and preparing legislation to give effect to the Constitution. The cases of the two Respondents are captured together in this judgment as they were represented and their cases presented by the same Counsel.

384. The 4th Respondent, Mr. Reuben Kimotho, relied on a Replying Affidavit he swore on 26th February 2019. The 7th Respondent on its part filed Grounds of Opposition dated 26th March, 2019.

385. Mr. Kimotho deponed that NIIMS is not replacing the current registration systems. On the contrary, in order to be enrolled on NIIMS, an individual is required to produce proof of registration with either an identification card issued by the 4th Respondent, a birth certificate issued by the Civil Registration Service; a Foreign National Identification Card issued by the Immigration Services or a Refugee Identification Card issued by the Refugee Affairs Secretariat.

386. Further, that the 4th Respondent is mandated by the Act to keep, in a register of all persons in Kenya to whom the Act applies, particulars of their registration number, name, sex, declared tribe or race, date of birth or apparent age, place of birth, occupation, profession, trade or employment, place of residence and postal address, finger and thumb impressions or palm and toe impressions, date of registration, and such other particulars as may be prescribed. It was his deposition that the impugned amendments made various minor amendments to the particulars to be kept in the register including the introduction of biometric data as part of the said particulars, and also established NIIMS. Mr. Kimotho averred that the Act grants the Director of the 4th Respondent the power and discretion to prescribe the manner in which the particulars are to be recorded, which cannot be taken away as proposed by the Petitioners.

387. It was his deposition further that it is apparent from the data capture tool that the information collected for purposes of NIIMS is information that is already in the custody of the 4th Respondent and other government agencies. Mr. Kimotho stated that in addition to the data capture tool, the government has also captured digital biometric data, namely fingerprints and facial features, for the purposes of NIIMS. He described NIIMS as a central database of digital photographs and digital fingerprints of Kenyan citizens and residents for purpose of integrating the personal information captured in the data capture tool to the biometric data. It was also his averment that NIIMS is aimed at integrating and consolidating information of the type already held by the 4th Respondent, with an individual's biometric data, for the purposes of creating, managing and operating a digitized national population register as a single source of personal information for all Kenyan citizens and residents. Mr. Kimotho averred that thereafter, each person will be assigned a unique national identification number known as the *Huduma Namba*.

388. He noted that this is an important departure from the current manual registration system identified in the Report by the Ministry of Information and Communication Technology in partnership with UNICEF, titled: **"Strengths, Weaknesses, Opportunities and Threats Analysis of Existing Identification and Registration Systems in Kenya, December, 2017"** and reiterated the gaps acknowledged by the Report as stated by the 2nd and 3rd Respondents. He further pointed out that birth registration and identity card systems are not synchronized, and the deployment of NIIMS would address this challenge.

389. Mr. Kimotho responded to various concerns about NIIMS raised by the Petitioners. In response to the contention that NIIMS is duplicating the functions of the Integrated Population Registration Service (IPRS) and lack of transitional provisions, Mr. Kimotho asserted that these two systems perform separate and distinct functions, and there is therefore no need for transitional mechanisms in the impugned amendments.

390. Mr. Kimotho explained that IPRS is a repository of information received from various registration agencies as a secondary source of personal information, and merely collates the said information with no point of contact with the subject of the information. That on the other hand, NIIMS provides the avenue for the collection of foundational information for all Kenyan citizens and residents directly from the owner of the said information. Further, that NIIMS integrates this foundational information with functional information held by other government institutions which IPRS does not do. It was therefore his averment that IPRS performs a passive function of merely receiving personal information from particular databases and storing them, while NIIMS performs the active function of collecting information first hand from the subject, and regularly integrates and updates the said

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 65 of 205.

information. Accordingly, that IPRS relies on data from other agencies while NIIMS relies on data received directly from the information subject.

391. Mr. Kimotho termed the allegation by the Petitioners that NIIMS would lead to infringement of the right to privacy as bare allegations. He stated that none of the Petitioners have set out with any degree of precision or specificity the manner in which this right has been violated, or is threatened with violation. It was his position that the petitions are based on abstract and hypothetical situations devoid of any real dispute. Accordingly, the allegation that the amendments in the Act that introduce Global Positioning System (GPS) as one of the particulars required in registration of citizens and residents is an infringement of the right to privacy is false and misleading. He further averred that GPS is merely a precise geographical location, expressed in longitude and latitude and only describes the precise location of a person's place of residence. He asserted that in any event, GPS is not currently being collected by the NIIMS data capture form in use.

392. Mr. Kimotho averred further that DNA as a unique identifier is not part of the personal information collected by the data capture tool. He, however, observed that the collection of DNA is an important tool in the prevention and investigation of crime and in curbing terrorism.

393. Regarding the contention that the impugned amendments seek to unnecessarily obtain personal information of Kenyan citizens and residents, and that the said information is not secure, Mr. Kimotho stated that information of a similar nature has been in the custody of the 4th Respondent in the exercise of its statutory functions. Furthermore, that this information is currently held in a "protected system" within the meaning of the Kenya Information and Communications Act and Computer Misuse and Cybercrimes Act and that the said Acts provide for penalties for offences involving protected computer systems.

394. It was his deposition further that NIIMS is operationalized under the Act and the information captured and stored therein therefore enjoys the protection of the provisions of sections 14 (1) (k), (l) & (m) of the Act which provided for penalties for unauthorized disclosure of the information. Moreover, that pursuant to sections 83G, 83H and 83I of the Kenya Information and Communications Act, personal information collected and held in the custody of the 4th Respondent is stored in electronic form. Mr. Kimotho cited various provisions of the Kenya Information and Communications Act and other instruments that safeguard the security and integrity of electronic records. He also deposed that adequate and effective administrative procedures, guidelines, custom and practices exist in the public service with respect to management of information held by government that guarantee security and integrity of that information. According to Mr. Kimotho, there has been no report of any compromise in the security of the digital records held by the 4th Respondent.

395. Mr. Kimotho denied the averments by the Petitioners that the data collection in NIIMS would be undertaken by a foreign corporation. It was his averment that on the contrary, it is only the biometric registration gadgets that were procured from a foreign firm as no Kenyan firm has the capacity to manufacture such gadgets. He averred that NIIMS was developed by the government of Kenya through the mandated Ministries, Departments and Agencies, and is therefore the intellectual property of the government. He asserted that the Petitioners had failed to demonstrate the inadequacy of the existing safeguards that protect personal information, and the manner in which the amendments to the Act violate the right to privacy.

396. On the concern raised by the Petitioners regarding vetting committees in the issuance of identity documents, Mr. Kimotho deposed that vetting is not a discriminatory process. Rather, it is an objective and verifiable process aimed at establishing the authenticity of a person's claim to Kenyan citizenship. Further, that vetting committees are established pursuant to the provisions of section 8 of the Act that give the 4th Respondent and its Director the power to demand proof of information and to establish identification committees or appoint persons as identification agents to assist in the authentication of information furnished by applicants and their parents or guardians. He explained that vetting committees are set up in respect of members of communities situate and present in Kenya, and also situate and present in other neighboring countries, because such border communities share physical features, culture and language with other communities outside the territory of Kenya.

397. While confirming that the vetting committees comprise various government officials, security agents and elders representing all communities in that locality, it was his averment that the vetting committees ensure inclusion of all communities, including Nubians. Mr. Kimotho averred that the guidelines on vetting set out the procedures and parameters to be considered to ensure that there is no discrimination. He was of the view that the principle of equality and non-discrimination permits the different treatment of people similarly placed if such treatment is meant to achieve a rational and legitimate purpose. Further, that the purpose of vetting is to ensure that only those with a legitimate claim to Kenyan citizenship are registered by the 4th Respondent, and the justification for the vetting of border communities is to address the influx into the country of the communities' counterparts from the neighbouring countries.

398. The 7th Respondent on its part stated in its Grounds of Opposition that the consolidated petitions were filed inordinately late since the impugned amendments were enacted in November, 2018. Its view was that if the orders sought are granted, they would occasion irredeemable and irreparable loss and damage to the State and to the citizens of Kenya who are in the process of implementing various provisions of the laws amended pursuant to the Statute Laws (Miscellaneous Amendment) Act No. 18 of 2018. Further, that the orders sought in the Petitions are contrary to public interest and the constitutional values of the doctrine of separation of powers as the legislative function is vested exclusively in Parliament and the Petitions request the court to substitute its views for those of Parliament. Lastly, that there is a general presumption of law that statutes enacted by Parliament are constitutional and the burden falls on the person who alleges otherwise to rebut this presumption, which burden has not been discharged.

The 5th Respondent's Case

399. The 5th Respondent is the Cabinet Secretary in the Ministry of Information, Communications and Technology (ICT), a public office established under the Constitution in the Executive arm of government. He is responsible for formulating, administering, managing and developing the government's information, broadcasting and communication policy, and is also the custodian of digital data collected and stored on behalf of the government.

400. The 5th Respondent filed a Replying Affidavit sworn on 26th February, 2019 by Jerome Ochieng, one of the two Principal Secretaries in the Ministry of ICT, who heads the State Department of ICT, Mr. Ochieng also swore several further affidavits on 26th April 2019 in response to affidavits and witness statements filed by the Petitioners and the 4th and 6th Interested Parties. The 5th Respondent also relied on the opinions of various experts, namely

Brian Gichana Omwenga, Muchemi Wambugu Edward and Mr. Loyford Muriithi, who all filed affidavits sworn on 14th May, 2019.

401. Mr. Jerome Ochieng gave a detailed background on the developments of the ICT sector in Kenya, including the initiatives at harmonisation of the population register, digitisation of data, and the development of policies and legislative frameworks. Some of the milestones he identified were the enactment of the Kenya Information and Communications Act in 1998 which has been variously amended thereafter, and the formation of an Inter-Ministerial Task Force on the creation of the Integration of Population Register System in September 2005.

402. Specifically with respect to NIIMS, Mr. Ochieng stated that in December, 2017, his Ministry, in partnership with the United Nations International Children's Emergency Fund (UNICEF) conducted a study on the **Strengths, Weaknesses, Opportunities and Threats Analysis of the Existing Identification and Registration Systems in Kenya**, which recommended the need for a '*single source of truth*' for citizen data. He averred that in furtherance of the mandate of the Ministry as described in Executive Order No. 1 of June 2018, a Cabinet Memorandum on the establishment of NIIMS was subsequently issued on 10th April, 2018. Under the said Cabinet Memorandum, the Ministry was charged with spearheading implementation of the NIIMS in collaboration with the Ministry of Interior and Coordination of National Government, and with operating the NIIMS infrastructure including the development of the necessary system design, integration structures, product identification and deployment.

403. To aid and facilitate this exercise, the Registration of Persons Act was amended by the Statute Law (Miscellaneous Amendments) Act No. 18 of 2018 to establish NIIMS. According to Mr. Ochieng, NIIMS is intended to be the primary database and "*single source of truth*" for personal data and will link and harmonise all the existing databases of personal information collected by different government agencies under different laws.

404. Mr. Ochieng asserted that his Ministry spearheaded the development of the software aspects of NIIMS with the input of other government agencies. He denied the contention by the Petitioners that private entities, particularly IDEMIA Saffron, was involved in the development of the software for NIIMS. Mr. Ochieng confirmed that the NIIMS kits were inspected for any data mining software to completely eliminate the possibility of external access, data mining or even data manipulation by IDEMIA Saffron or any other unauthorized entity.

405. It was Mr. Ochieng's deposition that NIIMS ensures the security of the nation from external and internal attacks since all persons in the country will be issued with relevant identifiers, including a unique number identifier from birth. He gave instances of the shortcomings of the current systems of registration, including those of access to documents and access to the registration systems themselves. He stated that NIIMS will reduce the duplication of processes common in accessing government services since it serves as a one-stop shop for identification information.

406. On the use of biometric data in NIIMS, Mr. Ochieng deposed that DNA as a unique identifier was not part of the personal information collected by the data capture form in use. He noted, however, that it plays a central role in the identification of individuals and is the only known means of posthumous identification in some instances. That notwithstanding, it was his averment that DNA, GPS coordinates, retina and iris patterns and earlobe geometry were not introduced by the impugned amendments. He averred that they were already
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 68 of 205.

provided for under section 5(1)(j) of the Act where it is provided that the Principal Registrar shall be required to keep “*such other particulars as may be prescribed*”.

407. Mr. Ochieng denied the allegations by the Petitioners that GPS targets an individual’s communication and exact whereabouts. He reiterated, like the other Respondents, that GPS is merely a precise geographical location, whose utility is to facilitate ease of digital identification of an individual’s place of residence and physical delivery of services to citizens by the government. He also echoed the other Respondents in asserting that GPS co-ordinates were not being collected by the NIIMS data capture tool. Accordingly, he averred that the alleged fears regarding the misuse of DNA and GPS coordinates is speculative, presumptuous, unjustified and misleading. It was his averment, however, that there will not be surveillance beyond the geographical location of residence.

408. Mr. Ochieng further deponed that there is an extensive existing legislative framework on the protection of privacy, personal information and integrity of ICT systems. He cited various provisions of the Access to Information Act 2016, the Kenya Information and Communications Act, and the Computer Misuse and Cyber Crimes Act, 2018 in support of this averment. Further, that there exists sufficient safeguards in respect of the security and integrity of information held by NIIMS in the said Acts, and in the Kenya Information and Communications (Consumer Protection) Regulations 2010. Mr. Ochieng explained that the country has a data protection policy which informed the development of the NIIMS software, and which has been reduced into a Data Protection Bill. Accordingly, that it is misleading for the Petitioners to allege that the exchange of data between agencies will expose them to intrusion.

409. Mr. Ochieng further contended that NIIMS is unlikely to face the shortcomings of the Ghana Card and India’s Aadhaar system given that the government has drawn vital lessons from some of the few errors made by the two systems. Furthermore, reports indicate that India and Ghana faced challenges in the implementation of their integrated information systems due to the fact that the registration exercises were carried out by private entities which created multiple data entries for financial gain. Further, NIIMS differs from Ghana’s Card and India’s Aadhaar system since the data capture software has been developed by the government, taking into consideration the country’s unique needs and aspirations. As such, it was of paramount importance that the government migrates to a single integrated database despite fears of technological failure which are in any case speculative and remote.

410. He further averred that in dealing with some of the challenges associated with developing new systems, the government organised several benchmarking trips to countries with similar systems, including Netherlands, Estonia, Malaysia, and the Philippines. Moreover, substantial public finances have been expended towards the deployment of NIIMS, and the orders sought by the Petitioners would run afoul of the principles of public finance enshrined in the Constitution. Mr. Ochieng averred that it would be unreasonable to establish and implement a system without learning from systems around the world and the NIIMS system has been hinged on extensive research on systems around the world.

411. It was his averment that globally, data is under constant and continuous threats of breach from criminal elements who seek to access and misuse it but, to mitigate this risk, there’s always a permanent surveillance, protection, update and upgrade of systems. He further averred that in establishing the NIIMS system, the State seeks to secure protection of national security, prevention and investigation of crime, especially in view of increasing terrorist

attacks in Kenya and heightened public safety concerns and provision and delivery of national services. Moreover, with present global trends in development, it is impossible to avoid digitization of information, even personal information, but the crux of the matter is in securing the data.

412. Mr. Ochieng averred that in any event, the registration was voluntary and all religious rights and beliefs were waived by those who profess them for the purposes of registration upon them weighing and finding that the system was satisfactory. He asserted that the Kenyan State will ensure that biometrics are only deployed when necessary and appropriate, and it is alive to its international obligations to respect human rights when collecting, processing, storing and sharing biometric information.

413. It was his position further that there are various security levels applied to protect data collected by the government to ward off any invader since the data is encrypted and access is restricted using highly sophisticated mechanisms that are almost impenetrable. According to Mr. Ochieng, the system's securities are designed to be in line with the international best practices guaranteeing confidentiality and integrity of data stored, and the system has undergone sufficient tests and trials and has shown itself to be resilient to attacks.

414. Mr. Ochieng averred that the Indian system was contaminated during the process of data collection. He disagreed with the 1st Petitioner's expert witness, Mr. Anand, asserting that it was not scientifically or academically sound or appropriate for the witness to quote his works and newspaper articles as authority on the propriety of the system he sought to criticize. The witness was also not, in his view, adequately grounded to swear on the facts of the system resources and infrastructure manned by the 5th Respondent for the protection of data. He noted that the company that Mr. Anand works for was one among many companies that could make suggestions on appropriate best practices and the 5th Respondent was not bound to take its suggestion.

415. Mr. Ochieng maintained, from his knowledge as an IT specialist, that the system is secure, not susceptible to breaches by malicious actors or abuse by public authorities, and undergoes constant surveillance, upgrades and updates by a competent team of men and women. Accordingly, the recent Marriott or Quora breach and India's Aadhaar's system cited by the Petitioners' witnesses are distinguishable from the system employed under NIIMS because their breaches are attributable to the operational mistakes where the persons collecting data were paid according to the volumes of people they registered, thereby placing data collection in the hands of commercial businessmen.

416. He therefore took the position that the allegations in the Petitions were unfounded, the Petitions lack merit and ought to be dismissed with costs.

417. Mr. Jerome Ochieng was cross examined on his affidavits by Mr. Waikwa and Mr. Awele, the respective Counsel for the 1st and 2nd Petitioners. He was questioned about his qualifications by Mr. Waikwa, which he highlighted as a Master's Degree in Information Engineering, a Bachelor's Degree in Maths and Computers, a Diploma in Management Information Systems and various professional courses on ICT. He also detailed his employment in government in various ministries and departments, including the ICT department. He confirmed that his understanding of NIIMS arises from his work and expertise, and also as a member of the Inter-ministerial Committee on NIIMS.

418. On the preparations and development of NIIMS, Mr. Ochieng stated that the discussions on NIIMS started in January 2018, and he referred to a copy of his letter dated 10th May 2018 inviting the technical committee on NIIMS to a meeting. He, however, clarified that the technical development of NIIMS commenced in February 2019 even though the preparations had started much earlier. He testified that the software for NIIMS was developed by Kenyans, and stated that tests had been done on algorithms to ensure they work, and on the system to verify its security and integrity, and ensure that there is no deduplication of data. He also explained that the data collected from NIIMS was currently not being utilized, in compliance with the orders of this Court, but that they had developed and tested the algorithms needed to utilize the data.

419. Mr. Ochieng confirmed that he knew of a company known as IDEMIA. He testified that the Ministry of Interior procured 31,000 registration kits in late 2018 from OT Morpho, which is now known as IDEMIA. He stated that the government cleaned the said kits in April 2019 before the start of the *Huduma Namba* registration exercise. However, that apart from procuring the kits from OT Morpho, the government did not engage the company in any other way in NIIMS.

420. Mr. Ochieng explained his understanding of the *Huduma Namba* and stated that it is a single source of truth, a place where one can find credible identification information about a person who seeks government services. According to Mr. Ochieng, the more data you have, the more credible the information on identity, hence his analogy of data to the new oil. On the SWOT report he annexed, Mr. Ochieng testified that if Kenya was to achieve a universal birth registration system that allocates a unique identifier to each child when it is born, then it would assist in personal identification. He denied that NIIMS overlaps this objective and stated that part of the motivation for NIIMS was from the SWOT report. He also testified that there was public participation in the development of NIIMS, and denied that it was only government and UNICEF officials who were involved in preparing the SWOT report.

421. Mr. Ochieng confirmed that the Data Protection Policy was approved by Parliament in 2019 and denied that it was prepared to frustrate the instant Petitions. He stated that there is no NIIMS policy in existence. He agreed with the objectives and benefits of NIIMS stated in Eng. Kibicho's affidavit and testified that NIIMS seeks to achieve inter-linkages and harmonization of different databases to address the challenges faced in identification. He disagreed that a longer time ought to have been taken to develop NIIMS, and stated that there is no time to consider alternatives due to the urgency for credible identification data.

422. When questioned by Mr. Waikwa on the law that regulates NIIMS, Mr. Ochieng responded that it is the Registration of Persons Act and that other than an executive Order on NIIMS, there are no rules on NIIMS. He also testified that delivery of services is not one of the purposes of NIIMS, and that there is no law that establishes the *Huduma Namba*. He explained that the term *Huduma Namba* is a communication concept for Kenyans to understand the nature of NIIMS as an integrated identity system, and denied that it was used to engage in a deception campaign and coerce Kenyans to register in NIIMS. He further testified that he was not aware of any law that regulates Article 31(c) of the Constitution, or creates the office of a Data Protection Commissioner or data controllers and processors.

423. Mr. Ochieng accepted that an identity card is required for registration for a *Huduma Namba* but denied that a Kenyan without an identity card would be filtered by the NIIMS system as a non-citizen. On the verification processes by NIIMS and the logs to the system by

other government agencies, he stated that it would be possible to tell where the interactions with the system occurred, and that the Access to Information Act regulates access to such metadata.

424. Mr. Waikwa concluded his cross-examination with questions on the NIIMS system design. The response from Mr. Ochieng was that NIIMS is a hybrid system that has interaction between a master database and functional databases. Further, that there will be no inter-linkages between the functional databases. He disagreed that the way of dealing with data breaches is to have a decentralised system or by minimization of data, but rather to have enough data and secure it. He however admitted that the design of NIIMS can still be technically changed.

425. On cross-examination by Mr. Awele, Mr. Ochieng testified that the existing registration databases are in the National Registration Bureau, the Immigration Department for passports and the Civil Registration Department. He stated that NIIMS introduces biometrical digital data because of the uniqueness of biometrics. He reiterated that the development of the NIIMS software was not an event but a process that started in 2018, before the enabling law was enacted.

426. Mr. Ochieng was cross-examined on the design and security of NIIMS, and stated that architecturally and technically, NIIMS has several layers. These are the data layer, the application system and the users layer, which all use encryption and are therefore adequately secured. Mr. Ochieng also stated that the report by Mr. Omwenga on **Government Wide Enterprise Architecture** was used as a guideline in the development of NIIMS and has not been formally adopted by the government. He admitted that the security policies of NIIMS have not been published, as this would compromise the system, and also that the public was not informed on the risks but only the benefits of NIIMS. Mr. Ochieng further stated that the Data Protection Policy guidelines as well as internal ministerial guidelines regulate the interoperability mechanisms and misuse of the data. He confirmed that the government had undertaken a Data Protection Impact Assessment of NIIMS whose report was not made public, and that an audit of the system is possible under the Access to Information Act.

427. During re-examination, Mr. Ochieng reiterated his evidence as to the nature of NIIMS and its benefits, its design, and the protection and security safeguards that are in place to protect the data collected by the system.

428. Mr. Brian Gichana Omwenga, the 5th Respondent's expert witness, deponed that he is a software and systems engineer and an Information Technology Consultant, holding a Master's Degree in Engineering Systems, Technology and Policy from the Massachusetts Institute of Technology (MIT), and is a Ph.D. Candidate in Computer Science. He also stated that he is a lecturer in Computer Science at the University of Nairobi and is the founding chairman of the Tech Innovators SACCO Ltd, an initiative that seeks to consolidate the Kenyan technology community through an empowered cooperative movement for the support of digital entrepreneurship. Further, that he is also the Chairman of the Industry Technical Committee that sets software and systems engineering standards at the Kenya Bureau of Standards (KEBS), and has previously worked in various capacities for Microsoft PLC, Nokia Research Africa, PricewaterhouseCoopers Kenya and Nokia Research Cambridge in Massachusetts, USA. Mr. Omwenga also averred that he has carried out various consulting assignments that have received several awards and global recognition and his research work has resulted in

various published papers and over ten (10) patents filed at the United States Patent and Trademark Office.

429. Mr. Omwenga averred that in 2017, he undertook research and authored a report titled **‘Government Wide Enterprise Architecture’**, which seeks synergies and efficiencies through combining common shared technical business services across government agencies and guides the journey of government’s digital transformation. Further, that this reduces costs by eliminating duplication of roles and efforts and promotes greater depth and expertise through the creation of centers of excellence for such shared business services. That subsequently, he was part of a team that carried out a feasibility study of the Government Enterprise Architecture and recommended various flagship projects including the unified unique digital identity project which was contained in a report titled **‘Digital Government Transformation Project.’**

430. Mr. Omwenga averred that identity, in relation to access and security, utilizes three common modes of authentication being something you *know* (such as a password), something you have (such as an access card) and something you are (such as biometrics) and any or all of the said three authentication modes may be incorporated in identity systems. However, the most robust factor of authentication and identification is based on something you *are*, that is, biometrics. It was also his averment that identity systems entail the maintenance of population registers which contain selected personal information (including biometrics) pertaining to each member of the resident population of a country in such a way as to provide the possibility of determining the identity of individual members comprising the population, the size of the population and the characteristics of such population.

431. Mr. Omwenga contended that the said population registers may either be centralized, decentralized or a combination of both, and could also be manual or electronic. He noted that the *United Nations Principles and Recommendations for a Vital Statistics System* provides that a population register need not take a specific form and states have unfettered discretion regarding the choice of the form, and the content of their respective population registers. It was his deposition that the rationale for this unfettered discretion is logically informed by the need to allow states to customize their respective population registers to suit their unique circumstances, which discretion enjoys adequate expression in international law. He cited Article 86 of the European Union General Data Protection Regulation 2016/679 (GDPR) which gives Member States the discretion to determine the specific conditions for the processing of a national identification number or any other identifier of general application.

432. In his view, capturing the value of good digital identity is by no means certain or automatic. Careful system design and well-considered government policies are required to promote uptake, mitigate risks like those associated with large-scale capture of personal data or systematic exclusion, and guard against the challenges of digital identity as a potential dual use technology. He stated that preconditions for digital identity include a minimal level of digital infrastructure, sufficient trust in the identity provider, and a policy landscape that provides safeguards to individuals. That in determining the content and the form of a population register, States take various factors into account including universality, accuracy and reliability, ease of operationalization, cost and security. Consequently, the form of an identity system that a State may opt to adopt may be a centralized identity system or a decentralized identity system or a combination of both.

433. It was his averment that a centralized identity system entails the maintenance of personal identity information of a country's population in one database (national master population register), whereas decentralized identity system entails the distribution of respective personal identity information in identity cards which are then issued to individuals. That a comparative analysis of the pros and cons of a centralized and decentralized identity system would weigh in favour of a centralized identity system for several reasons. First, that from a data security perspective, decentralized biometric identity systems are more susceptible to personal identity theft than centralized ones. He observed that a fake set of biometric features may easily be cast on a lost or stolen electronic identity card which is then used to facilitate identity theft.

434. Secondly, that from a cost perspective, it would be illogical and ineffective use of limited resources to facilitate the security of personal information stored in each electronic identity card issued to each individual citizen and registered foreign individuals resident in a country in question. He averred that centralization of identity data facilitates optimum allocation of resources by ensuring that a fraction of the limited resources are devoted to the sole security of a single database as opposed to millions of databases. Thirdly, that in any case, a decentralized biometric identity system would not dispense with biometric parameters such as fingerprints.

435. Mr. Omwenga further averred that NIIMS is neither entirely centralized nor entirely decentralized. This was because, first, the operationalization component of NIIMS is centralized in the sense that respective identities of individuals would have to be authenticated from one system as opposed to the current system where fragmented personal identities are respectively held in separate functional databases variously maintained by governmental ministries, departments and agencies (MDAs). Secondly, that NIIMS is decentralized to the extent that registrants will be issued with a card containing limited personal identity information such as unique identification number as opposed to biometric identity information hence the risk of identity theft attributable to decentralized systems is obviated. It was his averment therefore that a more accurate description of NIIMS would be an integrated identity system in which what is integrated is the identity data as opposed to functional databases variously maintained by MDAs. Accordingly, it is possible to maintain one population register in a number of digital copies at virtually minimal marginal costs and in the unlikely event of a breach on a copy of a digital population register, the other copies will remain unaffected.

436. Regarding the contents of population registers, Mr. Omwenga observed that it is impossible for individuals to prove their identities without providing sufficient personal information which include selected biometric and biographical information. That in deciding on the content of a population register, States are enjoined to balance two competing interests- the States' legitimate interest in maintaining a vital identity mechanism (based on biometrics) against the equally important interest in respecting the individuals' right to privacy. In his view, based on his knowledge and expertise, the processing of biometric data for purposes of establishment and operationalization of identity systems is not only justifiable under contemporary international law but is also a trite practice, world over.

437. It was his deposition that fingerprint matching has been used to identify individuals for thousands of years and across cultures. He further averred that an identity system that solely relies on the matching (deduplication) of one biometric feature is probabilistic as opposed to deterministic. However, combined with the matching of other biometric features and

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 74 of 205.

biographical data points (such as date of birth, facial image, parentage information, birth certificate, amongst others), it results in a multimodal identity system that is deterministic.

438. According to Mr. Omwenga, the probabilistic nature of individual biometric features justify the need for the requirement of multiple biometrics such as retina and iris patterns, hand geometry, earlobe geometry, voice waves and DNA in identity legislations, policies and systems. That the probabilistic nature of fingerprint matching (deduplication) is attributable to the fact that perfect matching of all data points in a fingerprint is not necessarily possible owing to extraneous factors. To increase the probability of a perfect fingerprint match, deduplication software is architecturally and functionally designed to keep templates of fingerprints of all available fingers of an individual. In his view, the NIIMS deduplication software is also designed as such. Accordingly, where a fingerprint is distorted, NIIMS would ideally have nine more sets of fingerprints with which to extract templates and run a match. In the unlikely event that all the fingerprints are distorted, or where an individual has none, the individual in question would not be disenfranchised in any way whatsoever because during the design of NIIMS, the probabilistic nature of fingerprint matching and the associated misgivings were anticipated and have been addressed by NIIMS in three ways.

439. He enumerated these as, first, for purposes of enrolment, in its current implementation design, NIIMS requires certain minimum data points from a potential registrant. These include the date of birth, parentage information, residence information, current national identification number for adult citizens, birth certificate in respect of children, and alien card number in respect of registered foreigners resident in Kenya, as well as facial image and fingerprints of all available fingers. Secondly, since some registrants may have distorted fingerprints, NIIMS has fingerprint-extraction software programmed to repair distorted fingerprints prior to either templatization or matching. Thirdly, where repair is impossible or where fingerprints are unavailable, other data points would, collectively, be used for purposes of uniquely identifying the affected individuals. He therefore deposed that no individual will be denied a *Huduma Namba* on account of either lack of, or distorted, fingerprints.

440. Mr. Omwenga expressed the opinion that the enrolment rejection of a genuine individual trying to enrol is a definite impossibility. In his view, associating NIIMS with India's Aadhaar is inaccurate based on the fact that the analysis by Mr. Anand and the conclusions derived therefrom were made on the unfounded assumption that NIIMS is architecturally and functionally similar to Aadhaar. Further, Aadhaar, as was described by Mr. Anand, is a singular identity system which relies, solely, on fingerprint matching. He noted that the analysis by Mr. Anand does not disclose whether there were corrective measures in place to remedy the alleged high rates of false rejections and false acceptance. Conversely, NIIMS is a multimodal identity system that relies on both biometric and biographical matching. Therefore, whereas Aadhaar is probabilistic, NIIMS is deterministic. He further averred that the said analysis disregards the inherent difference in both context and population demographics between India and Kenya, and neither does it take into account the operationalization difference between the implementation of NIIMS and the implementation of Aadhaar, that is while Aadhaar was commercialized, NIIMS was not.

441. According to Mr. Omwenga, ideally, multimodal identity systems such as NIIMS comprise several functional programmes that are variously derived from different source codes. However, the sensitive components of identity systems such as the various deduplication algorithms, encryption and decryption programmes, security programmes, amongst others, ought to be derived from closed source software as opposed to open source

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 75 of 205.

software regardless of the cost implication, for several reasons. First, sensitive programmes that run on open source software are vulnerable to cyber-attacks.

442. Secondly, open source software rides on the presumed goodwill of the coding community which assumption is flawed since open source software attracts all and sundry, including persons with malicious intent. A third reason is that closed source software fosters accountability unlike open source software which does not inspire accountability for the simple reason that the general public is a non-entity. Lastly, whereas the innovation cost of the open source software is borne by the general coding community, the costs attributable to additional services, assistance or added functionality are non-transferable and open source software is therefore not entirely free.

443. Mr. Omwenga further averred that NIIMS will only maintain a national master population register in electronic form, the NIIMS database and the type of personal information that will be kept in the said national master population register is expressly stipulated in the NIIMS digital data capture form and will be kept as encrypted templates. Therefore, without the requisite decryption key, a third party will not be able to unmask any encrypted personal information. That even if one was able to gain unauthorized access to the NIIMS database and unmask the personal information kept therein, it would be of insignificant commercial value. In his view, however, even if the purported ‘massive’ costs of data breaches were to be internalized, NIIMS would still pass a cost-benefit analysis.

444. With regard to the contents of Dr. Thomas Fisher’s affidavit, Mr. Omwenga observed that four (4) of the exhibits therein are authored by Privacy International which is not a party to these proceedings, and no evidence has been tendered to show whether the said documents have, at the very least, been peer-reviewed. Further, that the exhibit on the **United Nations Principles and Recommendations for a Vital Statistics System** is inapplicable to the issues of content, procedures, responsibilities and rights of data subjects, and the pros and cons of a national master population register. He observed that the World Bank Group has expressly disclaimed the findings, interpretations and conclusions expressed in the exhibit on **“Privacy Design: Current Practices in Estonia, India and Austria”** at the first page of the said document. It was therefore his averment that the said documents are devoid of probative value and any averments founded thereupon do not, as a matter of logic, rise to the status of independent expert opinion.

445. The Petitioners’ cross-examined Dr. Omwenga on his affidavit. During cross-examination by Counsel for the 1st Petitioner, Dr. Omwenga testified he was giving evidence as an expert for the government, for which he has done consultancies, but did not have a current contract with. He stated that his last contract with the government was in 2016 and 2017 when he undertook action research for the Government-wide Enterprise Architecture. It was his evidence that he had testified before as an expert in a number of cases by way of affidavit evidence for individuals but not for the government.

446. Mr. Omwenga testified that the 5th Respondent sought his expert advice, but that he had not tendered evidence of the technical specification of NIIMS. It was his testimony that he is well published but had not submitted any paper on NIIMS, and was not involved in building the technical aspects of NIIMS. He admitted that he knew of the existence of the Registration of Persons Act but was not conversant with its legal aspects. He further acknowledged not knowing who the administrator of NIIMS is.

447. Mr. Omwenga was shown Engineer Kibicho's affidavit sworn on 26th February 2019, and testified that he was in agreement with the fact that NIIMS will be a "single source of truth" on a person's identity. He maintained that from his experience and knowledge, NIIMS is neither a centralised nor decentralised system, and when asked about the nature of cards with biometric chips, he stated that they are decentralised as they are given to different individuals, and are not in a central database. He also stated that a central database would be multi-modal, and that for deduplication of the data in NIIMS, a set of algorithms will be needed to clean the data. He stated that a software engineer who has the capability and technology can develop algorithms, and gave his experiences developing algorithms in Kenya's 2017 elections. He further stated that there were many actors involved in developing the electoral system, and that OT Morpho was just one of many.

448. Dr. Omwenga testified that he is familiar with data protection policies, the concept of data minimization, and the concept of thresholds in both deterministic and probabilistic systems. In his view, data minimization is not only about counting data points but also about the quality of data being collected. Further, that more data collected about a person does not risk the subject's privacy, and collection of more data and the combining of biometric and demographic data is one of the ways of solving the problem of deterministic identity systems.

449. Dr. Omwenga stated that he had enrolled for the *Huduma Namba* using his identity card in order to be able to get government services. He, however, could not tell if he could have registered for it if he did not have his identity card. He conceded that though he had testified as a government expert, he had not tendered any evidence on the design and architecture of NIIMS. He maintained, however, that the more information NIIMS had the more accurate it would be, and DNA could be included as a means of identification.

450. Mr. Omwenga stated that he was not aware of the system being used to collect DNA currently. He however stated that NIIMS is deterministic and if one does not enrol to the system, one would not get a unique number. He did not, however, know if the system would require all documents such as the identity card and birth certificate in order for one to get a unique number.

451. In cross-examination by Mr. Awele, Counsel for the 2nd Petitioner, Mr. Omwenga stated that he had interacted with data protection several times in relation to data security in storage and in transactions, and he understood why it was important to protect data. He illustrated the importance of data protection and ownership of data by citing the work he had done on data protection and privacy for the Ministry of Health in the government enterprise architecture where it was clear that patients were still the owners of the data.

452. It was Mr. Omwenga's evidence that the consolidated Petitions raise legitimate concerns on security of the system, accuracy of NIIMS and misuse of data. He could not, however, confidently explain what NIIMS was since he was only involved in giving advice at the initial stage. His evidence was that it was the client, the Ministry of ICT, that was involved with designing NIIMS.

453. With respect to biometric registers, it was his evidence that he was only aware that the existing databases were only collecting fingerprints. He stated that he did not know the legal framework on NIIMS but he knew that some law brought it into existence. It was his testimony that the security, privacy and misuse concerns on NIIMS could be addressed if the recommendations he had already given to the government were used. His recommendation

entailed the use of a unique identifier on government enterprise architecture, security architecture and predefined security policies.

454. It was also his view that security systems should be predefined in some policy document, noting that some of the personal information to be collected by NIIMS is sensitive. He observed, however that not all information may require the same level of security and protection. It was his deposition that the implementation plans need to be kept secure to make the system secure, and the security process should be predefined so that data is not misused and someone who is not authorized does not access the data.

455. With regard to the issue of encryption of data, his evidence was that he did not know the encryption standard the government employed for the data collected in NIIMS. He further stated that if the government were to predefine its encryption standard for data it collects in NIIMS, it would address the Petitioners' concerns.

456. On re-examination by Dr. Nyaundi, and Mr. Njoroge Regeru, Mr. Omwenga emphasized that his role was advisory and that his report was not a NIIMS report, but made recommendations to be taken into consideration in the design of NIIMS. He reiterated his evidence on centralized and decentralised identity systems, and that centralized systems offer more protection to data. Further, that NIIMS is both an identity and identification system as the accuracy of its data on identity is what will aid in identification. Mr. Omwenga stated that NIIMS will have various identity attributes in a multi-modal way, and will be more deterministic than probabilistic. In conclusion, he stated that there is competence in our local professionals to design a system such as NIIMS, and denied that it is an archaic system.

457. The 5th Respondent's second expert witness, Muchemi Wambugu set out in his affidavit extensive details of his qualifications and experience. Of importance for present purposes is that he is a Management Consultant and founder of Sirius Consult which focuses on technology-led organizational transformations. Until 2016, he was a Partner in Technology Consulting Practice and the Advisory Leader for County Initiatives at Price Waterhouse Coopers, Kenya. He had also worked at Deloitte Consulting Ltd in Kenya and IBM Global Services in California, USA. He is therefore an accomplished ICT Management professional with more than 20 years of experience in advising both public and private organizations on business-centric ICT solutions, has extensive experience in global technology implementations, ICT transformation, strategy, operations, governance and programme and change management.

458. Mr. Muchemi averred that he undertook research and authored a report titled the **Strengths, Weaknesses, Opportunities and Threats Analysis of the Existing Identification and Registration Systems in Kenya, 2017** and had discovered several weaknesses regarding Kenya's identity systems. These were a lack of data harmonization; use of birth certificates numbers that do not uniquely identify individuals; duplication of data collection by government agencies; fragmented and uncoordinated registration and vital systems; untrusted relationship between the birth registration and the ID registration process; gathering of data in disparate and disjointed silos; systemic data corruption, data integrity and data quality issues. He had recommended in the said Report, among other things, addressing the gap in the data sharing protocols between government agencies, executing the government systems enterprise to allow for data access, security and governance in dealing with vital national data and the use of block chain to enhance data security.

459. It was also his averment that NIIMS was modeled from the Estonian identity system in so far as both systems respectively keep a centralized national master population register in digital form, and decentralized functional databases that are linked to the said national master population register. However, whereas the Estonian identity system utilizes PIN-codes that are embedded in electronic identity cards for purposes of authenticating identities of individuals, NIIMS utilizes unique identification numbers. Further, that electronic identity cards work for Estonia because Estonia is a homogenous country with a significantly lower population and an advanced e-government infrastructure. Kenya, on the other hand, is a heterogeneous society that experiences significant exposures from migration from troubled neighboring countries which, in some cases, have no control over terrorism and its effects on their neighbors. Therefore, a more robust identity system that suits the peculiar circumstances of Kenya is justifiable.

460. Mr. Muchemi further observed that fingerprint matching, in itself, is probabilistic as opposed to deterministic and no sole biometric identity matching is deterministic. However, an amalgamation of matching of various biometrics and biographical information results in a multimodal system that is deterministic. In his view, the operational and architectural design of NIIMS addresses the probabilistic nature of fingerprint deduplication in a number of ways. The first is that samples of fingerprints are extracted from all available fingers of an individual during data collection and each finger has an individual unique print character. Therefore, if one or two fingers fail, the other fingers can positively identify an individual.

461. Secondly, where an individual does not have fingers or in the unlikely event that all the fingerprints of an individual cannot be captured, other identity modes including facial image, date of birth, residence and parentage information would, collectively, be used to uniquely identify such individuals. This, in itself, increases the probability of perfect fingerprint matching. In his view, it is the amalgamation of the various probabilistic identity elements that make NIIMS deterministic.

462. It was his averment further that distortion of all fingerprints during an individual's lifetime on account of ageing, mutation or participation in manual labour is a rare occurrence because it is highly unlikely that one would come into contact with mutation-inducing radioactive materials in their lifetime. Secondly, manual labour is unlikely to cause distortion of all fingerprints of an individual's non-dominant hand. Further, that it is common scientific knowledge that human skin cells have a lifespan of a couple of months and are constantly replenished. In his view therefore, ageing does not distort an individual's fingerprints.

463. Mr. Muchemi deposed that during registration in multimodal identity system, biometric information and biographical information of an individual are captured, templated and stored in a national master population register. Secondly, before one is enrolled and thereafter issued with a unique identifier, his biometrics and biographical information is matched against the templates of individuals already registered in the aforesaid national master population register. Consequently, capturing a registrant's identity information and matching it against every other registrant's who has previously enrolled ensures that each person gets a single - one and only one - unique number and this verification procedure is impossible to attain in a non-digital system. Therefore *Huduma Namba* is a composite number that amalgamates the myriad of numbers that an individual citizen has from cradle to grave and will serve as a unique identifier to every citizen and registered foreign national resident in Kenya.

464. Mr. Muchemi further averred that inclusion of children in a national master population register is justified by the need for the government to offer service delivery more efficiently without prejudice to any section of its citizenry. He averred that infant biometric identification is now possible owing to technological advancement such as non-contact optical scanning technology that can uniquely identify infants at birth by imaging fingers and the palm of the hand. However, if for whatever reason, infant biometrics are unreliable, infants would still be sufficiently identified by connecting them to their parents who are themselves uniquely identifiable by their respective biometrics. It was his averment that for the purposes of resource allocation by government as well as accounting for all citizens for the purposes of service delivery, it is imperative to connect children to their parents. In his view, NIIMS could also help in the elimination of trafficking in children and child labour as well as help enforce laws against child marriage.

465. It was Mr. Muchemi's opinion that commercial tools may run on open source software primarily because of the commercial conveniences associated with open source software. However, government tools invariably run on closed source software owing to the nature of sensitivity of the information maintained and processed by such tools. Furthermore, systems that run on closed source software have their own security testing mechanisms. That regardless of the adequacy or lack of legislative and policy frameworks, sensitive systems such as NIIMS are architecturally designed to incorporate safeguards that guard the access of data even by authorized personnel to ensure that though they may access the data, they do not do it without accountability and that they can only access it when it is required. In any event, security of data in any digital system is not necessarily entirely dependent on the existence of stringent legislative and regulatory frameworks.

466. Mr. Waikwa, Counsel for the 1st Petitioner cross-examined Mr. Muchemi on his appointments to Boards of various organisations that have a connection with or are under the Ministry of ICT. Mr. Muchemi denied that he is a public officer, and stated that he has consulted for government, the last consultation having been in the SWOT analysis where he was seconded to UNICEF as the lead member for government. He clarified that his only connection with NIIMS was the SWOT report, which was prepared in December 2017 before the establishment of NIIMS, and that he had not conducted any study on NIIMS thereafter. He also testified that he is not involved in the implementation of NIIMS, nor in the setting up of the NIIMS architecture.

467. Mr. Muchemi stood by the averments in his affidavit on NIIMS being a centralized system, on the birth register being a unique identifier, and on probabilistic and deterministic system and deduplication and multi-modal systems, which he stated were reached from his SWOT analysis and his experience.

468. On re-examination by Dr. Nyaundi, and Mr. Njoroge Regeru, Mr. Muchemi clarified that he has professional involvement with corporate bodies and private sector bodies that work in the area of ICT, and that this did not influenced his SWOT analysis. Further, that the focus of the SWOT analysis was to harmonise fragmented citizens' identity information and that it did allude to a centralised database as a single source of truth on identity, which is NIIMS.

469. Mr. Loyford Muriithi also gave expert evidence on behalf of the 5th Respondent. He deposed that he is an Assistant Director in the Ministry of Information, Communications and Technology and has been involved in all the processes of development and establishment of

the NIIMS project. It was his testimony that in designing the operational and functional architecture of NIIMS, the government carefully selected various desirable attributes adopted by various jurisdictions they benchmarked in and customized them to suit the unique circumstances of Kenya. With particular reference to Estonia, he averred that the government consciously resorted to model its identity system from the Estonian one as both Kenya and Estonia keep a digital centralized master population register of all their respective citizens and registered foreign nationals and they have no monopoly over the individual functional data repositories that belong to the institutions linked to the said national master population registers.

470. As such, every institution linked to the national master population register can use the identity data kept in the national master population registers for purposes of authenticating the identity of individuals. However, the national master population registers can neither access nor use the functional data stored in the individual repositories belonging to the institutions linked to the national master population registers in question.

471. It was his deposition further that the departure of NIIMS from the Estonian system is marked by the fact that Estonia utilizes identity cards which are valid for both physical and digital identification and is based on an electronic chip and two pin codes supplied with the card. By using a smart card reader and a computer connected to the internet, citizens can use two core functionalities provided by the identity card, both of which are essential to the development of e-government.

472. The first PIN-code allows citizens to authenticate their identity so that the corresponding e-service knows the identity of the user. This is a first step that provides basic enabling infrastructure to provide personalized services and information via online means. The second PIN-code is used to sign documents or approve transactions online. Based on the foregoing, the authentication of an individual's identity in a digital environment in Estonia is dependent on what an individual has, a PIN code, as opposed to what an individual is, biometrics. Mr. Muriithi therefore averred that the inherent risk of an identity authentication based on what an individual has is not foolproof as anyone who accesses an individual's PIN-code can represent himself as being the individual in question, hence arrogate unto themselves the said individual's identity.

473. According to Mr. Muriithi, in order to avoid the risks inherent in the Estonian identity model, the government of Kenya consciously resorted to premise the authentication of an individual's identity, in a digital environment, on what an individual is, instead of what they have.

474. It was also his averment that whereas NIIMS uses data capture kits manufactured by IDEMIA/OT Morpho, it does not use any OT Morpho software. He averred that all the hardware components of NIIMS, including the data capture kits, were screened for any software including but not limited to data-mining software before their respective programming in Kenya. Further, all the registration and encryption programmes that run on the said hardware components of NIIMS were developed and installed locally by the government of Kenya. In the premises, NIIMS does not use OT Morpho deduplication algorithms.

475. It was also Mr. Muriithi's deposition that during the design architecture of NIIMS, the government of Kenya anticipated the possibility of certain individuals missing some biometric features or having biometric features that may not be captured by the biometric data

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 81 of 205.

capture kits. Accordingly, it adopted specific design features to obviate possible exclusion of such individuals and included the use of additional biometric features such as facial images and biographical information such as date of birth, parentage information, residency information, birth certificate serial number, national identity card number and alien card number to corroborate fingerprint matching; the digital capture of all the fingerprints from available fingers of an individual with a view to maximizing the probability of perfect fingerprint matching; and the use of dactyloscopic (fingerprint) experts to manually counter-check every enrolment rejected by the fingerprint deduplication algorithm on the basis of attempted multiple enrolment by the same individual. In the circumstances, it is highly unlikely that an individual may be denied enrolment in the national master population register on the basis of either missing fingers or having distorted fingerprints.

476. Mr. Muriithi further averred that being a multimodal identity system, NIIMS has several programmes that variously perform specialized tasks which collectively result in the creation of a digital biometric national master population register from which respective identities of individuals may be established with precision. Some of the said programmes were derived from open source software whereas some were derived from closed source software depending on the sensitivity of the tasks performed by the said programme(s) and the attendant procurement costs.

477. Specifically, the costly programme that perform non-sensitive tasks were derived from open source software, which explains why NIIMS data capture kits were programmed to run on android operating system. On the other hand, programmes that perform critical and highly sensitive tasks such as encryption and deduplication were derived from closed source software in respect of which the government of Kenya restricts the sharing, viewership and modification of the underlying source codes to essential personnel only. He expressed the view that it would therefore amount to veritable irresponsibility on the part of the Kenyan government to disclose, to the general public, the very codes that found the programme meant to guarantee the safety of personal data of its citizens and foreign nationals resident in Kenya.

478. As regards the Petitioners' concern on the security of the data, his averment was that the contents of the national master population register is limited only to the personal information that is sufficient to uniquely identify an individual and no more. This, he averred, is aptly manifested by NIIMS data capture forms. Further, that the purpose limitation and data minimization in the architectural design of NIIMS obviates the justification for the use of data for purposes extraneous to its originally intended purpose on account of its ready availability. Mr. Muriithi asserted that the personal information kept in the NIIMS database is secure because the moment the requisite biometric and biographical information is captured by the NIIMS data capture kits at the point of registration, the information is encrypted whether the data capture device is online or offline and the encrypted biometric and biographical information is transmitted, in encrypted form, to the requisite servers for deduplication. Further, the templates of biometric and biographical information stored in the NIIMS database are encrypted as well and in the premises, a data breach on NIIMS database would only reveal encrypted templates of personal identity information which cannot be unmasked without the requisite decryption key.

479. It was Mr. Muriithi deposition that the security of identity data is further guaranteed by the fact that the databases of the institutions linked to NIIMS database will only access NIIMS database for purposes of establishment of respective identities of individuals. Secondly, the functional data, such as criminal records, will remain resident in the respective

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 82 of 205.

repositories of the institutions that are linked to NIIMS database, in this case, the Directorate of Criminal Investigations database, and the NIIMS database cannot access the functional data variously stored in the said respective repositories of the institutions linked to NIIMS database.

480. It was his averment therefore that access to the NIIMS database would not provide the purported 360 degrees view of an individual's life alleged by the Petitioners. In his view, in the circumstances outlined above, there are sufficient technical safeguards that regulate the collection, processing, access and sharing of identity data by NIIMS. As regards children identity data, Mr. Muriithi averred that additional/special technical safeguards were incorporated in the architectural design of NIIMS database with a view to providing the requisite safety.

481. Mr. Muriithi was cross-examined by Hon. Martha Karua, the lead Counsel for the 2nd Petitioner, and Mr. Bashir, the Counsel for the 1st Petitioner. On examination by Hon. Karua, Mr. Muriithi confirmed that he was not part of the benchmarking team that went to other countries to study similar identity systems, but stated that he was involved in the design of NIIMS by adopting best practices from the benchmarking reports. He stated that the role of the ICT Ministry was to handle the technical issues and safeguards of the NIIMS, while the legal issues were handled by the business owner, which was the Ministry of Interior. He however stated that the ICT Ministry is the one that developed the Data Protection Policy and Bill.

482. He further testified that the technical safeguards are only known to the developers of the system, and that the safeguards they put in place for children was that their biometric data would only be captured from the age of six years. According to Mr. Muriithi, there are two levels of architecture of NIIMS. The first, which he termed the high level architecture, can be disclosed. However, that the second, which is the low level detailed architecture of the system, cannot be provided for security reasons.

483. Mr. Muriithi was cross-examined by Mr. Bashir on the sharing of data between NIIMS and other government agencies and functional databases. His view was that this would not be a good idea, and that there will be no back and forth sharing of data between the master database and the functional databases. Further, that there will be information flows to and from the master database to the functional databases in terms of queries, and on a needs basis determined by the institutional mandate. Mr. Muriithi stated that there will be mechanisms of recording who has accessed the system, but there is no system for citizens to know who has accessed their data. He reiterated that the intention of NIIMS is to authenticate the identity of all Kenyan citizens and foreigners by way of biometric data, and that no Kenyan citizen should be left out.

484. On re-examination by Mr. Nyaundi, Mr. Muriithi clarified that the high level architecture diagrams of the NIIMS system are pictorial representations with no source codes and which have little meaning to a technical person, while the low level diagrams are detailed with specifications and functionalities of every section of the system.

The 6th Respondent's Case

485. The 6th Respondent is the Speaker of the National Assembly, an *ex-officio* member of the National Assembly by dint of Article 97(1) (d) of the Constitution, and by dint of Article 107 of the Constitution, presides over sittings of the National Assembly. The 6th Respondent
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 83 of 205.

filed Grounds of Opposition all dated 20th February, 2019, a Replying Affidavit dated 28th February, 2019 and a Supplementary Affidavit dated 2nd May, 2019 all sworn by Mr. Michael Sialai.

486. Mr. Sialai averred that he is the Clerk of the National Assembly, an office in the Parliamentary Service Commission constitutionally mandated to run the operations and affairs of the National Assembly under Article 127 and 128 of the Constitution. It is further charged with providing technical and procedural advice to the Speaker and Members of the National Assembly on parliamentary practices and procedures.

487. In the Grounds of Opposition, the 6th Respondent contended that the Petitioners' actions were in bad faith as the impugned amendments were assented to by the President on 31st December 2018 and the Petitioners were therefore guilty of inordinate delay in instituting these proceedings which were time barred under the provisions of the Fair Administrative Action Act. Further, it was contended that the National Assembly's mandate to enact, amend and repeal laws is derived from the Constitution and the Petitions threaten the legislative role of Parliament and specifically the National Assembly's mandate under Articles 1(1), 94 and 95 of the Constitution. The 6th Respondent took the position that the Petitioners seek to restrict the National Assembly from carrying out its constitutional mandate derived from Article 95 (3) of the Constitution of enacting the impugned amendments.

488. It was also contended that the present Petitions contravene Article 109 of the Constitution which mandates Parliament to enact, amend or repeal any law through Bills passed and assented to by the President. The 6th Respondent asserted that there was adequate public participation in the process of enactment of the impugned amendments, but be that as it may, the process of enactment of legislation is not an administrative action falling within the purview of Article 47 of the Constitution or the Fair Administrative Action Act, 2015.

489. His contention was that in the context of legislation, what is required is that the legislature facilitates public participation on the Bill under consideration by the House. Further, that Article 94 (5) of the Constitution provides that only Parliament has the power to make provisions having the force of law in Kenya, and all the legislation passed by Parliament are presumed constitutional unless such presumption is rebutted. Accordingly, sections 3, 5 and 9A introduced to the Act through the impugned amendments are constitutional and properly enacted by the legislative arm of government and the burden falls on the person who alleges otherwise to rebut this presumption.

490. Mr. Sialai contended further that the process of national registration of persons is a policy decision solely within the mandate of the Executive and enacted by Parliament. He asserted that this Court is therefore ill-equipped to determine matters of policy, the economy and the proper mode of national registration process as the Petitioners ask the Court to do. In any event, according to the 6th Respondent, in determining the constitutionality of an Act of Parliament, the Court should look at the purpose and effect of the impugned statute and if the purpose and/or the effect of the statute do not infringe on a right guaranteed by the Constitution, the statute is not unconstitutional. In his view, the consolidated Petitions have not disclosed how the Constitution is violated by sections 3, 5 and 9A introduced to the Act through the impugned amendments.

491. In his affidavits, Mr. Sialai gave the chronology of events leading to the enactment of the impugned amendments. He averred that on Wednesday, 18th April 2018, the Statute Law (Miscellaneous Amendments) Bill (National Assembly Bill No. 12 of 2018) was introduced
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 84 of 205.

in the National Assembly. Thereafter, a motion of reduction of publication period from 14 days to 3 days was moved by Honourable Aden Bare Duale (the Member of Parliament for Garissa Township) in accordance with the National Assembly Standing Order 120, and the motion was passed by the House. On the same day, the Bill went through the first reading and was immediately committed to the National Assembly Departmental Committee on Administration and National Security to scrutinize by way of requesting for memoranda from the public as is mandated by Standing Order No. 127 (3) and Article 118 of the Constitution.

492. Mr. Sialai avers that on 7th May 2018, the National Assembly facilitated public participation on the Bill through print media by placing an advertisement in both the *Standard* and *Daily Nation* newspapers asking for memoranda from stakeholders. Thereafter, on 14th, 19th and 20th June 2018, the National Assembly Committee on Administration and National Security held stakeholders' meetings to which all stakeholders, including the Petitioners, were invited, to discuss the Bill, but they did not attend or submit a memorandum. It was his averment that it is therefore untruthful for the Petitioners to allege that there was no public participation.

493. According to Mr. Sialai, the public was involved in the process of enactment of the impugned amendments through invitations to make submissions and memoranda from stakeholders and the public meetings held on 14th and 19th June 2019. Consequently, the amendments introduced to the Act through the impugned amendments did not violate the principle of public participation under the Constitution. He drew attention to the fact that the Kenya National Commission on Human Rights, the 3rd Petitioner herein, in its analysis and review of the Bill dated 25th May, 2018 and published in its website, confirmed its approval of the amendments proposed with respect to the Act through the impugned amendments.

494. Mr. Sialai deposed that the National Assembly Committee on Administration and National Security compiled its report having taken into account the nature of the concerns raised by different stakeholders. This report was laid before the National Assembly on 3rd July, 2018. Thereafter, between Tuesday, 7th August 2018 and Thursday, 15th November 2018, the National Assembly, taking into account the concerns of the different sectors, considered and passed the impugned amendments and thereafter the Bill was forwarded to the President for assent in accordance with Article 115 of the Constitution. It was his position therefore that the impugned amendments were enacted in accordance with the Constitution and the National Assembly's Standing Orders and the National Assembly did not infringe any Article of the Constitution as alleged by the Petitioners.

495. According to Mr. Sialai, the amendments introduced to the Act could not be withdrawn to await the ongoing efforts to anchor them in substantive National Registration Identification Bill 2012 and the Registration and Identification of Persons Bill, 2014 (Senate Bill. No. 39), because the amendments introduced to the Act fell exclusively within the mandate of the National Assembly. This was on the grounds of its proper rubric, being a national legislation under Part 1 of the Fourth Schedule to the Constitution. It was also his contention that the purpose and intent of the impugned statute is stated in its Memorandum of Objects and Reasons clause which states that it is "*An Act of Parliament to amend the Law relating to Registration of Persons Act, to establish the National Integrated Identification Management System. The Bill proposes to provide for the capture of biometric data and geographical data in the registration of persons in Kenya*"

496. Mr. Sialai contended that in any event, matters of national registration and identification of persons are policy decisions solely within the mandate of the Executive and enacted by Parliament. In his view, the concerns raised against capture of biometric and geographical data in the registration of persons in Kenya as enacted in the impugned amendments are unjustified as the amendments are reasonable and justifiable in an open and democratic society.

497. He based this assertion on the argument that other modern and democratic countries such as Estonia, UK, Canada, Tanzania and Uganda have embraced the same model of national registration and identification of persons in order to address matters of national security and development. It was also his contention that matters of national registration and identification of persons are sanctioned by the Constitution and enactment of a law to regulate them cannot deprive the Petitioners of the right to privacy guaranteed under Article 31 of the Constitution. He further averred that the right to privacy is not absolute and is subject to reasonable restrictions in the public interest on grounds of national security, to preserve public order, to protect public health, to maintain moral standards, to secure due recognition and respect for the rights and freedoms of others or to meet the just requirements of the general welfare of a democratic society.

498. Mr. Sialai contended that these Petitions contravene the principle of presumption of constitutionality of legislation enacted by Parliament and are also a threat to the doctrine of separation of powers. He further contended that they are an encroachment on the legislative mandate of Parliament, and the orders sought by the Petitioners are tantamount to asking the Court to amend or repeal a piece of legislation. He therefore urged the Court not to exercise its discretion to grant the orders sought in the said Petitions as the Petitioners have not adduced any or any cogent evidence to demonstrate that their rights have been infringed by the enactment of the impugned amendments. His position was that the Petitions are devoid of merit, are frivolous, generally argumentative and an outright abuse of the court process and merely intended to stifle the 6th Respondent's mandate to legislate under the Constitution and ought to be dismissed.

499. In his Supplementary Affidavit, Mr. Sialai averred that during the process of the passage of the impugned amendments, each National Assembly Departmental Committee was tasked to examine each amendment as if they were distinct legislations. Further, in the advertisement calling for submissions to the various committees, each thematic area was distinctively before a relevant Departmental Committee in accordance with the Second Schedule of the National Assembly Standing Orders. Further, that the newspaper advertisement indicated which committee would deal with which subject matter in order to aid the public in presenting their views. It was also his averment that during the debates on the impugned amendments, Chairpersons of the respective committees were given time to indicate the views of the committees and those of the public. Further, that during committal in the House, Chairpersons of Committees were also required to move their respective amendments unlike in the past where this was done by the Justice and Legal Affairs Committee. According to Mr. Sialai, these were deliberate adjustment of rules of procedure to accommodate examination of the amendments by the House.

500. Mr. Sialai urged the Court to examine the Statute Law (Miscellaneous Amendments) Bill in the same manner as in the context of a Finance Bill which is passed every year by the National Assembly and whose intention is to amend several laws to deal with revenue-raising measures or even repeals in entirety certain taxation provisions in the law. He argued that the Petition 56, 58 & 59 of 2019 (Consolidated) | Page 86 of 205.

effect of a Finance Bill cannot be underrated to constitute an interpretation as minor amendments. It was his contention that this scenario applies also to a Statute Law (Miscellaneous Amendment) Bill whose intention is to amend many statutes. It contended that neither the Constitution nor the rules of the House bar Parliament from undertaking its legislative business using a Statute Law (Miscellaneous Amendment) Bill as long as the principles of public participation are adhered to.

501. According to Mr. Sialai, as a matter of Parliamentary practice, Parliament consolidates amendments due to either backlog of unlegislated areas or to save on Parliamentary time. He therefore argued that courts should let Parliament decide on its own nomenclature of Bills. It was his averment that the intent of the Statute law (Miscellaneous Amendments) Act No. 18 of 2018 was stated in the Memoranda of Objects and Reasons as being ‘*to make various wide-ranging amendments on various statutes*’.

502. He observed that the Supreme Court of Kenya in **Speaker of the Senate & Another v Attorney-General & 4 Others 2013** [eKLR] had recognized the power of the Houses of Parliament to establish and regulate their internal procedures without undue interference from courts. Further, the principle of separation of powers requires that there be mutual respect between the courts and the legislature, and that courts should exercise restraint when called upon to determine matters relating to the exercise of legislative power by Parliament, citing in this regard various decisions which we shall consider later in this judgment.

503. With regard to the challenge to the impugned amendments on the basis that they were not considered by the Senate, Mr. Sialai averred that the Statute Law (Miscellaneous Amendments) Bill (National Assembly Bill No. 12 of 2018), was not a Bill concerning counties. He cited the case of **National Assembly of Kenya & Another vs Institute for Social Accountability & 6 Others** (2017) eKLR in which the Court of Appeal held that in order for a Bill to qualify as a Bill ‘concerning county government’, the Bill must be one that affects the functions and powers of the county governments set out in the Fourth Schedule of the Constitution. In the circumstances, the procedure for the enactment of the impugned amendments was in line with the Constitution and the National Assembly Standing Orders. It was his position that for these reasons, this Court lacks grounds to invoke its jurisdiction under Article 165 of the Constitution to invalidate the legislation, and he urged the Court to dismiss the Petitions.

THE CASES OF THE INTERESTED PARTIES OPPOSING THE PETITION

504. In opposition to the Petition, the 1st Interested Party, Child Welfare Society of Kenya (CWSK), filed an affidavit sworn by its Chief Executive Officer, Irene Mureithi, on 27th March 2019. She described CWSK as a semi-autonomous government agency for the care, protection, welfare and adoption of children pursuant to Legal Notice No. 58 of 23rd May 2014.

505. Ms. Mureithi averred that she is aware that NIIMS as anchored in the impugned amendments integrates personal information with biometric and GPS data that shall, *inter alia*, enable the government identify precise geographical location of every citizen and resident of Kenya. She averred that whenever children are rescued by the government and placed in the custody of CWSK, its first task is to establish the identity of such children immediately. It is her position that NIIMS shall enable CWSK, which is duly established by the government as a national emergency response and rescue organization for children, to

identify lost and abandoned children as well as their families and unite them within the shortest time possible.

506. Ms. Mureithi deposed that NIIMS will assist the State in its constitutional mandate to protect children, its most vulnerable group, as required by the Constitution. In her view, the impugned amendments align the Act with the Constitution. She stated that CWSK, which is obligated by Legal Notice No. 58 of 2014 to strengthen families and provide families for separated children, children at risk of separation and children without appropriate care by facilitating local and international family tracing and reunification, will be aided by NIIMS in tracing thousands of separated children's families and confirming parentage in a manner that is faster, easier, cost-effective and friendly to a child and family.

507. Ms. Mureithi also asserted that pursuant to Article 53 of the Constitution, every child has a right to a name and nationality from birth; parental care and protection, which includes equal responsibility of the mother and father to provide for the child; and protection from abuse, neglect, harmful cultural practices, all forms of violence, inhuman treatment and punishments and hazardous and exploitative labour. She contended that any limitations imposed by the impugned law meets constitutional muster and are justified in an open and democratic society.

508. Her averment was that NIIMS shall facilitate with ease the tracing of families for separated children with special needs, which is often a challenge and deal with illicit adoption practices such as circumventing the process and forgery of documents which lead to child trafficking and permanent separation of children from their biological families. She further contended that the *Huduma Namba* will capture children's identity thereby curbing incidents where children are labeled as orphaned and abandoned when their biological parents are alive; curb change of children's identities and falsification of documents to change a child's name thereby preventing loss of identity; and assist in administration of social protection programmes for the most vulnerable group in society.

509. Ms. Mureithi also stated that from her experience, the process of tracing a child's family is usually tedious, lengthy and costly. Further, that DNA testing for children is done in circumstances that are psychologically overwhelming for the child and the parents. NIIMS, in her opinion, stands to assist in effectively tracing a child's family and confirm parentage without imposing unnecessary trauma to the involved parties, which includes children.

510. Ms. Mureithi averred that a special category of separated children are children with special needs and tracing their families is often a challenge. Further, that ensuring that separated children with special needs are placed in various forms of alternative family care equally becomes a challenge and almost impossible by reason of which some end up in institutions up to adulthood, thus denying them their constitutional right to parental care and protection. It was her position that through NIIMS, CWSK will be able to obtain each child's *Huduma Namba* and biometrics and mitigate against cases of children with special needs being abandoned and remaining in institutions for lengthy periods which is detrimental to their development.

511. Ms. Mureithi further argued that during political upheavals like the 2007-2008 post-election violence and natural calamities like drought or famine, children are usually separated from their parents. In her view, the implementation of the law would make reunification of children and their families take a shorter period.

512. Ms. Mureithi further averred that NIIMS stands to mitigate various crimes against children such as child labour. Through the available records of NIIMS, the children caught up in child labour and those at risk of entering child labour will be easily traced by the authorities. Further, that NIIMS will be able to track children attendance in schools and school dropouts, for instance how many children are accessing education in a given locality. It was her view that this information would be crucial for the government to ensure that various intervention programmes in the areas such as withdrawal and preventions of exploitation of children, especially in child labour, as well as provision of psychosocial support to ensure children are retained in schools are properly implemented.

513. Ms. Mureithi further contended that NIIMS will put an end to the cases of duplicate registration since the details of children will be captured and recorded from birth. It was her averment that at the moment, a child can acquire various aliases which end up registered at various levels. She further contended that as the system is very porous, it makes it easy for networks and conspirators to traffic a child especially in a commercialized legal process. She argued that DNA biometrics will easily lead to reunification of children with their birth families, while through NIIMS, children from border communities who are in the country for one reason or the other will be identified and monitored. Referring to **The Trafficking in Persons Report 2017** by the Department of State of the United States of America (USA), she stated that currently, Kenya is cited as a source, transit and destination country in human trafficking.

514. Ms. Mureithi further stressed the benefits of NIIMS, contending that the process of advertising children for tracing is costly and lengthy, and with the advent of NIIMS, these costs will be reduced drastically and the time taken will be minimal. She noted that Kenya is a signatory to the Hague Convention on Inter-country Adoption which provides for the subsidiarity principle which implies that in cases of children who have no parents, all local options should be exhausted before considering inter-country adoptions. It was her contention that NIIMS shall aid in ensuring due diligence in terms of finding local options for a child such as opportunities for family preservation as opposed to exiting Kenyan children to foreigners while many Kenyans are ready and willing to support their own. CWSK therefore urged the court to dismiss the Consolidated Petitions.

515. The 8th Interested Party, International Policy Group, opposed the petition through an affidavit sworn on 26th April, 2019 by its Director, Dr. Kenneth Orengo. Dr. Orengo's averment was that as per Sustainable Development Goals (SDGs) set by 150 nations, including Kenya, at the 4th plenary meeting of the United Nations General Assembly held on 25th September, 2015, the provision of legal identity for all, including birth registration, was identified as one of the goals to be attained by 2030. He averred that sustainable development and the objectives of the SDGs form some of the national values and principles of governance under Article 10 of the Constitution.

516. Dr. Orengo stated that following the adoption and ratification of the SDGs in 2015, various multilateral and international organizations, including the World Bank, UNDP and UNICEF, have undertaken significant work and deployed resources to facilitate implementation of the goals. These organizations, of which Kenya is a member, have all stressed the critical role played by digital identity databases in realizing the SDGs. He cited in support of this averment the statement by the World Bank in its April 2015 report titled **'Digital IDs for Development: Access to Identity and Services for All'** that official identification is more than a convenience; that it is a fundamental human right and is

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 89 of 205.

indispensable for connecting residents to electoral participation, educational opportunities, financial services, health and social welfare benefits, and economic development. He further deposed that it gives people a chance to better communicate with and be recognized by their government while giving governments the opportunity to listen and improve the lives of their citizens.

517. Dr. Orengo also cited a report titled **'The Role of Identification in the Post-2015 Development Agenda'** issued by the World Bank on 1st April, 2015 where it was stated that the ability to prove one's identity is a cornerstone of participation in modern life and is basic to many of the rights set out in the Universal Declaration of Human Rights and the Convention on the Rights of the Child, which rights include the right to a name, a nationality and to recognized family relationships on both the paternal and maternal sides. He noted that in its report titled **'Principles on Identification For Sustainable Development: Toward The Digital Age'** issued on 2nd February, 2018, the World Bank had once again observed that living without proof of legal identity is a serious obstacle to social, economic, and political inclusion, and that it also makes it difficult for an individual to open a bank account, vote, obtain formal employment, access education or healthcare, receive a social transfer, buy a SIM card, or seek legal redress.

518. Dr. Orengo further noted the observations in the report that a person without identification may be unable to exercise the full range of human rights set out in international laws and conventions. Further, that weak civil identification systems also represent challenges for countries such as governance planning, service delivery, public sector administration, collecting taxes, border control and emergency response. He averred that the World Bank had also noted that the move towards digital platforms by public and private service providers can increase efficiency of service delivery, create significant savings for citizens, governments, and businesses by reducing transaction costs, as well as drive innovation. This can generate many benefits but can also exacerbate the risk of isolation for poorly-connected populations including rural and remote communities, the forcibly displaced, stateless persons and other marginalized groups.

519. The final report cited in support of the 8th Interested Party's statement that digitization of identity is unstoppable is the research by McKinsey Global Institute in January 2019 titled **'Digital Identification: A Key to Inclusive Growth.'** The report indicates that the Institute had found that digital identification has the potential to unlock economic value equivalent to 3 to 13percent of GDP in 2030, assuming high adoption rates. Further, the research also established that beyond quantifiable economic benefits, digital identification can offer non-economic value to individuals through social and political inclusion, rights protection and transparency. It noted that robust identity programmes can help guard against child marriage, slavery, and human trafficking.

520. It was Dr. Orengo's position that the right digital identification technology, designed with the right principles and enforced with the right policies such as those formulated in Kenya, can protect individuals from the risk of abuse and enable the safe inclusion of billions in the digital economy.

521. The 8th Interested Party stated that by providing greater legal protection, digital identification can help in the elimination of child labor, currently estimated to affect 160 million children, by providing proof of age; fight child trafficking; help enforce laws against child marriage and thus contribute to its elimination; and contribute to the empowerment of

women and girls worldwide. Dr. Orengo cited the case of Indonesia in which 95% of girls who married at 18 years of age or younger lacked a birth certificate.

a) It was the 8th Interested Party's case that digital identification has three benefits. The first was time and cost savings. Mr. Orengo stated that institutions using high-assurance identification for registration could see up to 90% cost reduction in customer on-boarding, with the time taken for these interactions reduced from days or week to minutes by enabling streamlined authentication to improve the customer experience in digital channels. The second benefit lay in fraud savings. It was averred that digital identification can help reduce fraud in a wide range of transactions, from decreased payroll fraud in worker interactions to reduced identity fraud in consumer and taxpayer and beneficiary interactions. A third benefit lay in increased tax collection. It was its position that greater revenue facilitated by digital identification could expand the tax base, helping promote formalization of the economy and more effective tax collection. Its position was that emerging economies, in particular, could experience substantial benefits.

522. Dr. Orengo also averred that the *Huduma Namba* generated by NIIMS will greatly deter payroll fraud known locally as the "ghost workers" problem which has been afflicting management of public funds in Kenya for several decades. He cited digital listing of police officers as having weeded out nearly 2600 ghost workers in the police force, saving the country approximately Sh1.7 billion in future annual wages.

523. It was Dr. Orengo's statement that a digital identification system such as the *Huduma Namba* can also unlock non-economic value, potentially furthering progress toward ideals that cannot be captured through quantitative analysis, including those of inclusion, rights protection and transparency. It was his view that such a system can promote increased and more inclusive access to education, healthcare and labour markets; can aid safe migration and can contribute to greater levels of civic participation. Further, that such a system is an indispensable tool in assisting the State to progressively implement Article 43 of the Constitution which is practically impossible to implement without accurate and credible data. It was also his averment that a digital identification system such as *Huduma Namba* can help enforce rights nominally enshrined in law. He illustrated this contention with the case of India, stating that the right of residents to claim subsidized food through ration shops is protected because their identity and claim is authenticated through a remote digital identification system, rather than at the discretion of local officials.

524. Dr. Orengo also deposed that transparency is another benefit of a digital identification system such as *Huduma Namba*. He contended that an accurate, up-to-date death registration system can help to curb social protection fraud, and that a reliable authentic voter registry is essential to reduce voter fraud and ensure the overall integrity of the electoral process. He gave an example of Pakistan as having updated its voter rolls with strong biometric controls that resulted in the inclusion of an additional 36 million new eligible voters as well as the elimination of 13 million entries with invalid identities, 9 million duplicates and 15 million entries without verifiable identities. He contended that a verifiable unique number that includes biometric markers, such as *Huduma Namba*, should not only address the accuracy and credibility of the voters register once and for all but also save the country billions of shillings that are used every 5 years to clean up the voters register and register new voters.

525. According to Dr. Orengo an integrated digital identification can also be used in the provision of e-government services and benefits, expanding access and saving time for

citizens while reducing costs for governments and improving social welfare, when compared to existing physical touch points. His view therefore was that the benefits of an integrated digital identification programme far outweighed violation of individual privacy rights for which adequate remedies are provided in law. Further, that the risks associated with digital identification systems can be mitigated.

526. On the requirement of GPS coordinates by the impugned law, Dr. Orengo deposed that this is not anything new but has in fact been a requirement of the Land Registration Act and the Land Act since 2012 when the two statutes were enacted as law without any opposition from the Petitioners or any other Kenyans. He cited various sections of the said land laws in support of his statement.

527. Stating that the risks to data security and the right to privacy can be mitigated, Dr. Orengo argued that the right to privacy must often be balanced against the State's compelling interests, including the promotion of public safety and improving the quality of life. He averred that in February 2018, United Nations agencies and human rights organizations that specialize in privacy rights issues met and formulated a set of common principles fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks. He enumerated some of the principles that were formulated as including, first, ensuring universal coverage for individuals from birth to death, free from discrimination, while the second principle was removing barriers to access and usage and disparities in the availability of information and technology. The third principle requires States to establish a robust, unique, secure, and accurate identity, while the fourth requires creating a platform that is interoperable and responsive to the needs of various users.

528. A further principle, according to the 8th Interested Party, is using open standards and ensuring vendor and technology neutrality, protecting user privacy and control through system design, planning for financial and operational sustainability without compromising accessibility, and safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. Other principles are establishing clear institutional mandates and accountability, and finally, enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

529. Dr. Orengo deposed that he was aware that Kenya already has or is in the process of enacting several provisions in statutes that protect the right to privacy and conform to the principles on data security and privacy, which he set out in his affidavit. It was his averment that despite a massive and aggressive negative propaganda campaign mounted by the Petitioners in the media, close to 20 million Kenyans had nevertheless registered with *Huduma Namba*, which showed that Kenyans had confidence in the digital identification system.

530. Edward Kingori, a member of the Terror Victims Support Initiative, the 9th Interested Party swore an affidavit on 26th April, 2019 in which he joined the Respondents in opposing the Petitions. He averred that the 9th Interested Party is a group formed to assist victims of terrorist attacks in Kenya and give them a forum to share their experiences, support each other and engage the government on the eradication of terror attacks in the country.

531. Mr. Kingori averred that a citizen's right to privacy must be limited as privacy can be an avenue for terrorists and their sympathizers and financiers to disguise their identity and subsequently afford them an opportunity to meet, plan, and finance attacks in the guise of right to privacy. He deposed that allowing terrorists unlimited rights is equal to surrendering

the right to life as the terrorists' rights cannot be more important or so precious that their rights should not be limited.

532. Mr. Kingori listed in his affidavit several incidents of terror attacks that have occurred in Kenya. He averred that terrorists and criminals are, by the very nature of their activities, faceless and shadowy figures who go to great lengths to hide and misrepresent their intentions, plans and activities. It was, he asserted, a utopian fantasy to insist that law enforcement agencies should rely on the old paper based methods of fighting such criminals or that settled notions of human rights protection such as *habeas corpus*, the right to bail and the right to privacy apply to terrorists. Further, that apart from maiming and loss of lives, terrorist acts have also had a negative effect on many sectors of the economy especially those involved in the hospitality sector which in turn feeds into a vicious cycle of collapsing hotel businesses with the attendant job losses and entrenched poverty in places like the former Coast province. His opinion was that the *Huduma Namba* will be a useful tool in fighting terrorism.

533. Mr. Kingori deposed at length on the legislative measures taken by Kenya and other jurisdiction in the fight against terrorism. It was his averment that those laws have limited the right to privacy but such limitation has been found to be constitutional. The case of **Coalition for Reform and Democracy (CORD) & 2 others vs Republic of Kenya & 10 others** [2015] eKLR was cited as upholding the limitations imposed on the right to privacy by the National Intelligence Service Act as reasonable and justifiable on account of the circumstances facing the nation.

534. It is the 9th Interested Party's case that the use of integrated databases, including DNA databases, is now one of the most effective tools in fighting crime, especially crimes involving violence, terrorism and sexual offences. He gave the United States of America and South Africa as examples of countries with DNA databases. Mr. Kingori, however, conceded that those databases are reserved for those who come into contact with the law and not the general population.

535. The 9th Interested Party contended that the Consolidated Petitions are predicated on the theory that governments should be treated with suspicion or are not to be trusted with data or are incapable of responsibly dealing with data. He noted that, conversely, millions of Kenyans have entrusted their most private data with private social media entities including Facebook, Twitter, Tinder and Google who retain such data in cloud repository servers, and Mr. Kingori wondered why the Petitioners have not lifted a finger against such foreign entities.

536. It was his deposition that as at 24th April, 2019, more than 15.6 million people had voluntarily registered with the NIIMS system across the country. That the process had also received broad bipartisan support across the political divide, which confirmed that the people of Kenya had given a vote of confidence to NIIMS. He therefore urged the court to dismiss the Consolidated Petitions.

ANALYSIS AND DETERMINATION

537. We have considered the pleadings of the parties as well as their detailed respective submissions and authorities, and have identified three substantive issues for determination:

i. Whether the legislative process leading up to the enactment of Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 was constitutional. In this regard, three sub-issues arise:

b. Whether enactment of the impugned amendments vide a Statute Law (Miscellaneous Amendments) Bill was procedural and/or appropriate in the circumstances;

c. Whether the Statute Law (Miscellaneous Amendments) Bill 2018 was a Bill concerning counties and should therefore have been subjected to approval of the Senate.

ii. Whether the amendments to the Registration of Persons Act through the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 violate and/or threaten violation of the right to privacy contrary to Article 31 of the Constitution. In this regard, four sub-issues arise:

a. Whether the personal information collected pursuant to the amendments to the Registration of Persons Act is intrusive, excessive and disproportionate to the stated objectives of NIIMS;

b. Whether the rights of children to privacy are violated or threatened with violation by the impugned amendments;

c. Whether there are sufficient legal safeguards and data protection frameworks for the personal information that is collected in NIIMS;

d. Whether the impugned amendments to the Registration of Persons Act are an unreasonable and unjustifiable limitation to the right to privacy.

iii. Whether the amendments to the Registration of Persons Act through the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 violate and/or threaten violation of the right to equality and freedom from discrimination contrary to Article 27 of the Constitution in respect of Nubians and other marginalised communities.

538. These Consolidated Petitions therefore raise procedural issues related to the process of enactment of the Statute Law (Miscellaneous Amendment) Act 2018 as well as substantive concerns related to the question whether the impugned law violates or threatens to violate constitutional rights. We shall begin our analysis by considering the procedural questions related to the enactment of the impugned amendments, then the question whether the impugned law violates or threatens to violate the constitutional right to privacy guaranteed under Article 31, and finally, whether the impugned amendments violate or threaten to violate the right to non-discrimination guaranteed under Article 27 in so far as the rights of the Nubian community and other vulnerable groups are concerned.

539. However, before we enter into an analysis of the issues, we deem it necessary to consider the question as to whether this Court has jurisdiction, and if so, the applicable constitutional and other principles that guide this Court in the exercise of its jurisdiction.

The Court's Jurisdiction

540. The 6th Respondent has attempted to ward off the court's inquiry into the issues raised by the Petitioners by flashing the separation of powers card and asserting the principle of parliamentary privilege. It has told the court that it should not touch the impugned amendments as that would amount to interference with the National Assembly's constitutional mandate to legislate. Our response to these arguments is that there is a plethora

of authorities which confirm that Parliament can only successfully raise the defence of separation of powers or parliamentary privilege by proving compliance with the Constitution and the law. Anything done by Parliament outside the confines of the Constitution and the law attracts the attention and action of this court. In conducting an inquiry into the constitutionality of the decisions and actions of the legislature the Court finds constitutional authority in Article 165(3)(d).

541. In its decision in the case of **Council of Governors & 6 others vs Senate** [2015] eKLR, the court expressed the ambit of this mandate as follows:

“We are duly guided and this Court vested with the power to interpret the Constitution and to safeguard, protect and promote its provisions as provided for under Article 165(3) of the Constitution, has the duty and obligation to intervene in actions of other arms of Government and State Organs where it is alleged or demonstrated that the Constitution has either been violated or threatened with violation....To our mind, this Court has the power to enquire into the constitutionality of the actions of the Senate notwithstanding the privilege of inter alia, debate accorded to members of the Senate. That finding is fortified under the principle that the Constitution is the Supreme Law of this country and the Senate must function within the limits prescribed by the Constitution. In cases where it has stepped beyond what the law and the Constitution permit it to do, it cannot seek refuge in illegality and hide under the doctrine of parliamentary privilege....In that regard, we have already found that the Constitution is the supreme law of the land and all state organs have an obligation to uphold it and the Senate must always act in accordance with the Constitution. Its procedures and resolutions must be made within the purview of the same constitution and it cannot purport to violate the Constitution and seek refuge in the doctrine of separation of powers. This Court, under Article 165(3) (d) (ii) of the Constitution is constitutionally mandated to examine whether anything done under the authority of the Constitution is well within the four corners of the Constitution. The Senate cannot therefore act in disregard of the Constitution and at the same time claim to exercise powers under the same Constitution. This Court will continue to exercise its jurisdiction and judicial authority as conferred by the people of Kenya to assert the authority and supremacy of the Constitution and when the Senate has violated the Constitution, it must be told so.”

542. In its decision in **In the Matter of the Speaker of the Senate & another** [2013] eKLR, the Supreme Court confirmed this principle when it held that:

“It emerges that Kenya’s legislative bodies bear an obligation to discharge their mandate in accordance with the terms of the Constitution, and they cannot plead any internal rule or indeed, any statutory scheme, as a reprieve from that obligation. This Court recognizes the fact that the Constitution vests the legislative authority of the Republic in Parliament. Such authority is derived from the people. This position is embodied in Article 94(1) thereof. The said Article also imposes upon Parliament the duty to protect the Constitution and to promote the democratic governance of the Republic. Article 93(2) provides that the national Assembly and the Senate shall

perform their respective functions in accordance with the Constitution. It is therefore clear that while the legislative authority lies with Parliament, the same is to be exercised subject to the dictates of the Constitution. While Parliament is within its general legislative mandate to establish procedures of how it conducts its business, it has always to abide by the prescriptions of the Constitution. It cannot operate besides or outside the four corners of the Constitution. This Court will not question each and every procedural infraction that may occur in either of the Houses of Parliament. The Court cannot supervise the workings of Parliament. The institutional comity between the three arms of government must not be endangered by the unwarranted intrusions into the workings of one arm by another....Where the Constitution decrees a specific procedure to be followed in the enactment of legislation, both Houses of Parliament are bound to follow that procedure. If Parliament violates the procedural requirements of the supreme law of the land, it is for the courts of law, not least the Supreme Court to assert the authority and supremacy of the Constitution.”

543. The Petitioners contend, among other things, that the process of the enactment of the impugned amendments violated the Constitution. It is therefore our sacrosanct duty to determine whether that allegation is true, and if so, provide appropriate remedy. Our fidelity to the Constitution and by extension to the people of Kenya, from whom our mandate emanates, cannot be shaken by isolated reference to the doctrine of separation of powers. The Constitution must be read as a whole. Whereas the Constitution recognizes the doctrine of separation of powers, the same instrument mandates this court to determine whether any action undertaken by Parliament violates the Constitution or the law. That the Constitution should be read as one document finds support in the case of Tinyefuza vs Attorney-General, Const. Pet. No. 1 of 1996 (1997 UGCC3), in which the Ugandan Court of Appeal held that:

“[T]he entire Constitution has to be read as an integrated whole and no one particular provision destroying the other but each sustaining the other.”

544. We find no reason to expound further on the jurisdiction of this Court in so far as the enforcement and protection of the Constitution is concerned.

Applicable Constitutional Principles

545. It is also useful, before embarking on an analysis of the issues, to set out and bear in mind the principles applicable in a matter challenging the constitutionality of legislation. The starting point is Article 259(1) which obliges this Court to interpret it in a manner that promotes its purposes, values and principles, advances the rule of law and the human rights and fundamental freedoms in the Bill of Rights, permits the development of the law and contributes to good governance.

546. In determining whether an impugned legislation or action is unconstitutional, the provisions of the Constitution must be interpreted purposively in line with Article 259(1) and other principles of constitutional interpretation. In the case of Institute of Social Accountability & Another v National Assembly & 4 Others High Court, [2015] eKLR, the court summed up these principles as follows:

[57] “[T]his Court is enjoined under Article 259 of the Constitution to interpret the Constitution in a manner that promotes its purposes, values and

principles, advances the rule of law, human rights and fundamental freedoms in the Bill of Rights and that contributes to good governance. In exercising its judicial authority, this Court is obliged under Article 159(2)(e) of the Constitution to protect and promote the purpose and principles of the Constitution. In determining whether a statute is constitutional, the court must determine the object and purpose of the impugned statute for it is important to discern the intention expressed in the Act itself (see Murang'a Bar Operators and Another v Minister of State for Provincial Administration and Internal Security and Others Nairobi Petition No. 3 of 2011 [2011]eKLR, Samuel G. Momanyi v Attorney General and Another (supra)). Further, in examining whether a particular statutory provision is unconstitutional, the court must have regard not only to its purpose but also its effect...

[59] Fourth, the Constitution should be given a purposive, liberal interpretation...Lastly and fundamentally, it is the principle that the provisions of the Constitution must be read as an integrated whole, without any one particular provision destroying the other but each sustaining the other (see Tinyefuza v Attorney General of Uganda Constitutional Petition No. 1 of 1997 (1997 UGCC 3)). We are duly guided by the principles we have outlined and we accept that while interpreting the impugned legislation alongside the Constitution, we must bear in mind our peculiar circumstances. Ours must be a liberal approach that promotes the rule of law and has jurisprudential value that must take into account the spirit of the Constitution."

547. Similarly, the Canadian Supreme Court stated in R v Big M Drug Mart Ltd., [1985] 1 S.C.R. 295 that:

'Both purpose and effect are relevant in determining constitutionality; either an unconstitutional purpose or an unconstitutional effect can invalidate legislation. All legislation is animated by an object the legislature intends to achieve. This object is realized through impact produced by the operation and application of the legislation. Purpose and effect respectively, in the sense of the legislation's object and its ultimate impact, are clearly linked, if not indivisible. Intended and achieved effects have been looked to for guidance in assessing the legislation's object and thus the validity.'

548. The Constitution should also be interpreted in a holistic manner that entails reading one provision alongside other provisions, and considering the historical perspective, purpose, and intent of the provisions in question. In Re the Matter of Kenya National Commission on Human Rights [2014] eKLR, the Supreme Court considered the meaning of "a holistic interpretation of the Constitution," and stated:

"[26] But what is meant by a 'holistic interpretation of the Constitution'" It must mean interpreting the Constitution in context. It is the contextual analysis of a constitutional provision, reading it alongside and against other provisions, so as to maintain a rational explication of what the Constitution must be taken to mean in light of its history, of the issues in dispute, and of the prevailing circumstances. Such scheme of interpretation does not mean

an unbridled extrapolation of discrete constitutional provisions into each other, so as to arrive at a desired result.”

549. Courts have consistently affirmed that a holistic interpretation of the Constitution calls for the investigation of the historical, economic, social, cultural and political background of the provision in question. This view was expressed by the Supreme Court in Communications Commission of Kenya & 5 Others v. Royal Media Services Limited & 5 Others, [2015] eKLR, that:

“the Constitution should be interpreted in a holistic manner, within its context, and in its spirit.” The Supreme Court in interpreting the *Constitution took into consideration the historical, economic, social and political background* of the Articles it had been called upon to consider.”

550. In The Speaker of The Senate & Another vs. Honourable Attorney General & Others, [2013] eKLR, Mutunga, CJ, cited with approval the holding in Tinyefuza v Attorney General Const Petition No. 1 of 1996 (1997 UGCC3) that:

“[184] The entire Constitution has to be read as an integrated whole, and no one particular provision destroying the other but each sustaining the other. This is the rule of harmony, rule of completeness and exhaustiveness and rule of paramountcy of the written Constitution.”

551. Article 24 sets out the principles that a court should consider in an analysis of the question whether legislation, which is challenged on the basis that it limits fundamental rights in the Bill of Rights, meets the requirements of the Constitution. It provides as follows:

24. (1) A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including—

(a) the nature of the right or fundamental freedom;

(b) the importance of the purpose of the limitation;

(c) the nature and extent of the limitation;

(d) the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and

(e) the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose.

(2) Despite clause (1), a provision in legislation limiting a right or fundamental freedom—

(a) in the case of a provision enacted or amended on or after the effective date, is not valid unless the legislation specifically expresses the intention to limit that right or fundamental freedom, and the nature and extent of the limitation;

(b) shall not be construed as limiting the right or fundamental freedom unless the provision is clear and specific about the right or freedom to be limited and the nature and extent of the limitation; and

(c) shall not limit the right or fundamental freedom so far as to derogate from its core or essential content.

(3) The State or a person seeking to justify a particular limitation shall demonstrate to the court, tribunal or other authority that the requirements of this Article have been satisfied.

552. The Petitioners, particularly the 1st Petitioner, allege violation of constitutional rights, specifically the right to equality and non-discrimination, and the right to privacy under Article 31 of the Constitution. Accordingly, a burden is placed on them to demonstrate, with a reasonable degree of precision, the manner in which their rights or the rights of others under these provisions of the Constitution have been or are threatened with violation. They are required to set out precisely the Articles of the Constitution alleged to have been infringed and the manner of such infringement-see Anarita Karimi Njeru vs Republic [1979] 1 KLR 154.

553. In Trusted Society of Human Rights Alliance vs Attorney General and 2 Others [2012] eKLR, the Court re-affirmed the holding in the Anarita Karimi Njeru Case and stated that:

“We do not purport to overrule Anarita Karimi Njeru as we think it lays down an important rule of constitutional adjudication; a person claiming constitutional infringement must give sufficient notice of the violations to allow her adversary to adequately prepare her case and to save the court from embarrassment on issues that are not appropriately phrased as justiciable controversies. However, we are of the opinion that the proper test under the new Constitution is whether a Petition as stated raises issues which are too insubstantial and so attenuated that a court of law properly directing itself to the issue cannot fashion an appropriate remedy due to the inability to concretely fathom the constitutional violation alleged.

The test does not demand mathematical precision in drawing constitutional Petitions. Neither does it require talismanic formalism in identifying the specific constitutional provisions which are alleged to have been violated. The test is a substantive one and inquires whether the complaints against the Respondents in a constitutional petition are fashioned in a way that gives proper notice to the Respondents about the nature of the claims being made so that they can adequately prepare their case.”

554. It is the principles that emerge from the cases cited in the preceding sections and the analysis required of the court from the provisions of Article 24 set out above that shall guide our determination of the constitutional issues that arise in these Consolidated Petitions.

Use of Expert Evidence

555. A second set of principles that should guide the court relates to the use of expert testimony by the parties given that all the parties relied on expert witnesses in support of their respective cases. Submissions were made, particularly by the 5th Respondent, on the nature of Petition 56, 58 & 59 of 2019 (Consolidated) | Page 99 of 205.

the expert evidence and the circumstances under which the Court should place reliance on such evidence. The 5th Respondent requested the Court to find persuasion in the evidence of its expert witness, Mr. Brian Omwenga, who undertook research and authored a report titled **‘Strengths, Weaknesses, Opportunities and Threats: Analysis of the Existing Identification and Registration Systems in Kenya, 2017’**.

556. In this report, according to the 5th Respondent, its expert recommended remedial measures to address the gap in the data sharing protocols between government agencies and the execution of the report on **Government Wide Enterprise Architecture** to allow for data access, security and governance in dealing with vital national data. Further, that the NIIMS system was part of the recommendations by the expert. The 5th Respondent contends that, on the other hand, the Petitioners’ expert witnesses had not interacted with the NIIMS system, and their knowledge of the alleged flaws in it was hypothetical and speculative.

557. The 5th Respondent cites the decision in **Stephen Kinini Wang’onduru vs The Ark Limited [2016] eKLR** and **Kimatu Mbuvi T/A Kimatu Mbuvi & Bros vs. Augustine Munyao Kioko [2007] 1 EA 139** on the consideration of, and weight to be given to, expert testimony by a court. In particular, it submits that expert evidence should not trump all other evidence; that it should not be considered in a vacuum and that it should be evaluated in the context of other evidence. Therefore, that even though experts are called upon to assist the court to evaluate complex matter, the said evidence is not compelling on its own.

558. This Court received *viva voce* evidence from expert witnesses, who provided the Court with important information. Under section 48 of the Evidence Act, opinions of science or art are admissible if made by persons specially skilled in such science or art. The said section provides as follows:

“(1) When the court has to form an opinion upon a point of foreign law, or of science or art, or as to identity or genuineness of handwriting or finger or other impressions, opinions upon that point are admissible if made by persons specially skilled in such foreign law, science or art, or in questions as to identity, or genuineness of handwriting or fingerprint or other impressions.

(2) Such persons are called experts.”

559. The first requirement therefore, of a party who calls an expert witness, is to establish the credentials of the person as an expert, or one who is especially skilled in that branch of science or art, to the satisfaction of the Court. The question whether a person is specially skilled within the meaning of section 48 of the Evidence Act is a question of fact that has to be decided by the Court, and failure to prove the competency of a person a party calls as an expert presents a real risk of evidence of such a person being ruled out as irrelevant.

560. The 5th Respondent alleges that the Petitioners’ expert witness was not specially skilled on NIIMS as he had not interacted with it. We note that from his qualifications, the Petitioner’s expert witness, Mr. Anand Venkatanarayanan holds a Bachelor’s degree in Technology with Computer Science Major from the University of Madras and he stated that he was an expert Cyber Security and Computer fraud forensic analysis. He also had work experience as a software engineer from June 1998 to August 2018, a period of 20 years. In our view his training and experience makes him specially skilled in computer systems, and to

this extent, his evidence was relevant. His lack of interaction with NIIMS in our view will only be pertinent to the import of any conclusions he makes on the issues before this Court.

561. The import of an expert's conclusions in this respect is influenced by the overriding consideration that an expert's opinion is based on facts. Because of that, the expert must either prove by admissible means the facts on which the opinion is based, or state explicitly the assumptions as to fact on which the opinion is based. In addition, the expert witness ought to explain the reasoning behind his opinion and the basis of the reasoning. Lastly, while the opinion of the expert is relevant, the decision must nevertheless be the judges'.

562. The weight to be attached to such an opinion by the Court would depend on various factors. These include the circumstances of each case; the standing of the expert; his skill and experience; the amount and nature of materials available for comparison; and the care and discrimination with which he approached the question on which he is expressing his or her opinion, as noted by a five judge bench of this Court in **Mohammed Ali Baadi & Others vs The Attorney General & 11 Others** (2018) e KLR. The said five judge bench held as follows on the factors the court will take into account when deciding what weight to be given to expert evidence:

“Firstly, expert evidence does not “trump all other evidence.” It is axiomatic that judges are entitled to disagree with an expert witness. Expert evidence should be tested against known facts, as it is the primary factual evidence which is of the greatest importance. It is therefore necessary to ensure that expert evidence is not elevated into a fixed framework or formula, against which actions are then to be rigidly judged with a mathematical precision

Secondly, a judge must not consider expert evidence in a vacuum. It should not therefore be “artificially separated” from the rest of the evidence. To do so is a structural failing. A Court's findings will often derive from an interaction of its views on the factual and the expert evidence taken together. The more persuasive elements of the factual evidence will assist the Court in forming its views on the expert testimony and vice versa. For example, expert evidence can provide a framework for the consideration of other evidence.

Thirdly, where there is conflicting expert opinion, a judge should test it against the background of all the other evidence in the case which they accept in order to decide which expert evidence is cogent and give reasons why the court prefers the evidence of one expert as opposed to the other. Fourthly, a judge should consider all the evidence in the case, including that of the experts, before making any findings of fact.”

563. Reliance was placed by the Court on various decisions including **Ndolo vs Ndolo**, (1996) eKLR, **Kimatu Mbuvi T/A Kimatu Mbuvi & Bros. vs Augustine Munyao Kioko** (2006) eKLR and **Huntley (also known as Hopkins) (a protected party by his litigation friend, McClure) vs. Simmons** [2010] E.W.C.A. Civ. 54. It was also noted that where there is a conflict between experts on a fundamental point, it is the Court's task to justify its preference for one over the other by an analysis of the underlying material and of their reasoning, and that a Court may find that an expert's opinion is based on illogical or even irrational reasoning and reject it, and may give little weight to an expert's testimony where it finds the expert's reasoning speculative or manifestly illogical and as a result unreliable. The

various expert testimony presented before us shall therefore be analysed on the basis of the above principles.

564. We now turn to consider the substantive issues raised in the Petition.

Whether the Legislative Process was Constitutional

565. The first issue to consider relates to the question whether the legislative process leading up to the enactment of the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 was constitutional. In addressing this question, we consider whether the impugned amendments were subjected to public participation in accordance with the Constitution, whether the enactment by way of an omnibus Statute Law (Miscellaneous Amendment) Act was procedural or appropriate in the circumstances, and finally, whether the impugned law was a Bill concerning counties and should therefore have been subjected to approval of the Senate.

Whether there was Public Participation.

566. The Petitioners contend that the enactment of the impugned amendments did not comply with the constitutional requirement for public participation. The 1st Petitioner submits that apart from a call to the public to give views on the Statute Law (Miscellaneous Amendments) Bill 2018, no information was made available to the public as to what NIIMS was, what it would entail, its potential vulnerabilities, and how it would affect the lives of Kenyans and foreign nationals resident in Kenya. It submits that the right to public participation is intertwined with the right to information since, for adequate participation to take place, those participating must have the salient information necessary to intelligibly form and articulate their opinion on what is proposed. The 1st Petitioner cites the decision in the case of **Katiba Institute vs President's Delivery Unit & 3 others** [2017] eKLR as stating that successful and effective public participation in governance largely depends on the citizen's ability to access information held by public authorities, and the right to access information becomes a foundational human right upon which other rights must flow.

567. The 1st Petitioner takes the view that in enacting the impugned amendments, the National Assembly was bound by the national values and principles of public participation, transparency and accountability. Article 118 of the Constitution is cited as requiring Parliament to conduct its business in an open manner, including opening its sittings and those of its committees to the public. To buttress this argument, it relies on the case of **Law Society of Kenya vs Attorney General & 2 Others** [2013] e KLR (hereafter the **2013 Law Society Case**) in support of the statement that in order to determine whether there has been public participation, the court is required to interrogate the entire process leading to the enactment of the legislation. According to the 1st Petitioner, the court in **Law Society of Kenya vs Attorney General & Another** [2016] eKLR (hereafter the **2016 Law Society Case**) also held that any amendments introduced on the floor of the House subsequent to public participation ought not to be completely new provisions which were neither incorporated in the Bill as published, nor the outcome of the public input.

568. The 1st Petitioner further relies on the case of **Kenya Human Rights Commission v Attorney General & Another** [2018] eKLR in which the South African case of **Matatiele Municipality & Others vs The President of South Africa & Others(2)** (CCT 73/05 A [2006] ZACC12; 2007 (1) BCLR 47 (CC) is cited for the proposition that the Constitution contemplates that the people will have a voice in the legislative organs of the State, not only through elected representatives but also through participation in the law-making process. The

1st Petitioner also cites the case of **Robert N. Gakuru & others v Kiambu County Government & 3 others**[2014] eKLR (the **Robert Gakuru Case**) as highlighting the ingredients of the kind of engagement with the people that will pass constitutional muster. It notes that in **Kiambu County Government & 3 Others v Robert N. Gakuru & Others**[2017] eKLR, the Court of Appeal held that the people must be accorded an opportunity to participate in the legislative process, and it was upon the party that was required to comply with this constitutional requirement to prove that indeed there was compliance.

569. It is the 1st Petitioner's submission that in the words of Ngcobo, J **Doctors for Life International vs. Speaker of the National Assembly and Others (CCT12/05) [2006] ZACC 11; 2006 (12) BCLR 1399 (CC); 2006 (6) SA 416 CC** (the **Doctors for Life Case**) merely allowing public participation in the law-making process is not enough but more is required, and measures need to be taken to facilitate public participation. The 1st Petitioner concludes its arguments on the issue by asserting that, as stated in the **2016 Law Society Case**, failure to comply with this obligation renders the resulting legislation invalid.

570. The 1st Petitioner's submission on the issue of public participation is linked to the claim that there was insufficient information on NIIMS. The 1st Petitioner submits that given the significant implication of NIIMS, the national government had a duty to disclose the information in order to allow the public to understand what was being proposed, how it would affect their lives and to make an informed decision whether the proposal was reasonable or not. It is also the 1st Petitioner's view that the National Assembly had a concomitant duty to provide the public with all the information relating to the implication of the impugned amendments, including the legal effects and the changes to be achieved through NIIMS. The case of **Nairobi Law Monthly Company Limited vs The Kenya Electricity Generating Company & 2 others** [2013] eKLR is cited in support of the importance of access to information, as it is at the core of the exercise and enjoyment of all other rights by citizens. Further, that the right to information does not only imply the entitlement by the citizen to information, but also imposes a duty on the State to provide information. Also cited in support of this position is the decision in the case of **Mohamed Ali Baadi and others vs Attorney General & 11 Others** [2018] eKLR.

571. The importance of the right to access information is further stressed by reference to the South African case of **The President of RSA v M & G Media** [2010] ZASCA 177, in which the Supreme Court of Appeal stated that open and transparent government and free flow of information concerning the affairs of the State is the lifeblood of democracy. Also cited is the case of **RSA v. M & G Media** (CCT 03/11) [2011] ZACC 32, where the Constitutional Court of South Africa noted that the constitutional guarantee of the right of access to information held by the State gives effect to "accountability, responsiveness and openness".

572. Another decision that was cited is that of **Claude-Reyes et al. vs Chile** (September 19, 2006) where the Inter-American Court of Human Rights explained that the right to access information is critical in auditing whether State actions are performed in accordance with the law. Further, that the State's actions should be governed by the principles of disclosure and transparency in public administration, to enable its subjects to question, investigate and consider whether public functions are being performed adequately. Relying on the above decisions, the 1st Petitioner submits that the Respondents have not provided any evidence that information was ever provided to the public, especially at the stages when public views could have affected or informed the government plans on NIIMS.

573. Like the 1st Petitioner, the 2nd Petitioner also alleges non-compliance with the Constitution and the law in the enactment of the impugned amendments. Referring to the provisions of Articles 10(2)(a) and 118(1)(b) of the Constitution and Standing Order No. 127(3) of the National Assembly Standing Orders which provide for public participation in the legislative process, the 2nd Petitioner opines that these provisions essentially represent the expanded scope of our democracy to make it partly representative and partly participatory. It is its submission that these provisions have been interpreted as conferring a positive and mandatory duty on the National Assembly to take deliberate, positive and genuine measures to facilitate meaningful, informed and quality participation by ordinary citizens in its legislative processes.

574. According to the 2nd Petitioner, the legislature is also expected to ensure that views that may influence any legislation are taken into account before any such law is passed. The 2nd Petitioner asserts that public participation promotes openness, transparency and accountability, which are the foundational tenets of a constitutional democracy. In that regard the **Robert Gakuru Case** is cited as aptly capturing the centrality of public participation in Kenya's legislative processes. The decision is also relied upon in support of the statement that public participation ought to be real and not illusory, and ought not to be treated as a mere formality for the purposes of fulfillment of the constitutional dictates.

575. The **Doctors for Life Case** is identified as underlining the standard and quality of public participation. Relying on the said case, the 2nd Petitioner submits that public involvement in the legislative process requires access to information and the facilitation of learning and understanding in order to achieve meaningful involvement by ordinary citizens. Further, that the legislature should create conditions that are conducive to the effective exercise of the right to participate in the law-making process.

576. According to the 2nd Petitioner, the nature of the legislation and its effect on the citizens plays a role in determining the degree of facilitation that is reasonable and the mechanisms that are most appropriate to achieve public involvement. The case of **Matatiele Municipality & Others vs The President of South Africa & Others (Supra)** is cited in support of this statement. The 2nd Petitioner argues that the alleged public participation prior to the enactment of the impugned amendments was cosmetic, and well below the constitutional standard laid out in the **Robert Gakuru Case**. It is the 2nd Petitioner's observation that the Constitution and the Standing Orders of the National Assembly require more than mere advertisement in a newspaper in view of the fact that the impugned amendments impact on every sphere of the day to day lives of the public thus affecting citizens' fundamental rights.

577. In order to demonstrate the absence or inadequacy of public participation, the 2nd Petitioner asserts that the stakeholders meetings that were purportedly held on 14th, 19th and 20th June 2018 were in actual fact internal parliamentary proceedings attended by parliamentary staff within Parliament buildings, and were out of reach to ordinary citizens. Further, that no evidence was adduced of actual invitations to the public or other stakeholders to those meetings. It is therefore the 2nd Petitioner's conclusion that the said meetings fell short of the standard of public participation, and the impugned amendments therefore violated Articles 10(2)(a) and 118(1)(b) of the Constitution.

578. It is further the submission of the 2nd Petitioner that the advertisements in the newspapers inviting members of the public to submit representations on the impugned law as a whole were themselves cosmetic. It contends that the said adverts failed to comply with the

mandatory provisions of Article 24(2)(a) of the Constitution that require that any legislation limiting a constitutional right must specifically express the intention to limit that right or fundamental freedom, and the nature and extent of the limitation. Its view is that had the requirement been complied with, there could have been greater participation by the public.

579. The 2nd Petitioner also takes issue with the seven days given to the public to provide their views. Its position is that the public was given seven days to submit representations on proposed amendments to 68 Acts, but no effort was made to provide any information. It contends that there was no memorandum or explanation setting out the scope, effect and objects of the impugned amendments to enable the public make informed representations. According to the 2nd Petitioner, no input was expected from the public in such circumstances.

580. Further, that considering the nature, importance, intensity and impact of the impugned amendments on the public, seven days was an unreasonably short period to expect any person to appreciate the full import of the impugned amendments, and to submit any meaningful representations thereon. It is the 2nd Petitioner's contention that there was no attempt to exhort the public to participate in the process of the enactment of the Bill. The 2nd Petitioner therefore concludes that the impugned amendments failed constitutional muster as they were passed in violation of Articles 10(2)(a) and 118(1)(b) of the Constitution and are accordingly liable for invalidation.

581. The 3rd Petitioner was in consonance with the other Petitioners in faulting the impugned amendments for non-compliance with the constitutional and statutory requirements for enactment of laws. The 3rd Petitioner asserts, firstly, that the impugned amendments were passed without the input of the public. It cites the Doctors for Life Case for the proposition that public participation in the conduct of public affairs ensures that citizens have the necessary information and avails them an effective opportunity to exercise the right to political participation. Also cited is the case of Poverty Alleviation Network & Others vs President of the Republic of South Africa & 19 others, CCT 86/08 [2010] ZACC 5, which was cited with approval in Kenya Small Scale Farmers and Others vs Republic and Others Nairobi [2013] eKLR on the essence of public participation, and for the observation that a decision that is made without consulting the public can never be an informed decision.

582. According to the 3rd Petitioner, neither the public nor stakeholders were invited to submit their memoranda or to participate in the public hearings held by the National Assembly. Further, that the public was not sensitized on the contents of the impugned amendments and their effects. The 3rd Petitioner relies on the case of Minister of Health and Another vs New Clicks South Africa (Pty) Ltd and Others 2006 (2) SA 311 (CC) in support of the proposition that what matters is that at the end of the day, a reasonable opportunity is offered to members of the public and all interested parties to know about the issues and to have an adequate say; and that what amounts to a reasonable opportunity will depend on the circumstances of each case.

583. The 3rd Petitioner submits that the court must look at the entire process to determine whether it meets constitutional muster and relies in support on the 2013 Law Society Case. The 3rd Petitioner's conclusion is that the process of passing the impugned amendments was fundamentally flawed as the public was unable to submit memoranda due to the short notice, and that there was no invitation to either present the memoranda or for public hearings.

584. The Interested Parties who support the Petition also hold the view that the manner of the enactment of the impugned amendments render them unconstitutional. They support the Petition 56, 58 & 59 of 2019 (Consolidated) | Page 105 of 205.

Petitioners' claim that public participation was insufficient. The 5th Interested Party cites the case of **Kenya Union of Domestic, Hotels, Education and Allied Workers (Kudheha Workers) vs Salaries and Remuneration Commission (2014) e KLR** where the court held that the Constitution, at Article 94, has vested legislative authority of the people of Kenya in Parliament, and that Article 118 has provided for public participation and involvement in the legislative business. It opines that introducing amendments that are controversial and substantive through an omnibus Amendment Act limits the ability of persons to participate. Its view is that in the instant case, the general public only had 8 days to go through the entire miscellaneous amendment Bill that was introducing amendments to the impugned Act and 66 other statutes. In its view, even for the most elite members of society, this was an unconscionable burden.

585. It is also the case of the 5th Interested Party that there was no mention of the mandatory collection of personal information by the State to aid in the functioning of NIIMS. There was therefore, in the 5th Interested Party's view, an entire facet of issues left out when the public was invited to give their views on the Bill. It is the 5th Interested Party's position that the public participated without information, and their participation was therefore not as meaningful as it would have been had the public been made aware of the entirety of what NIIMS was to entail. The 5th Interested Party cites the case of **Lucy Wanjiru & another vs Attorney General & another [2016] eKLR** which quotes the case of **Secretary, Ministry of Information and Broadcasting Government of India & Others vs Cricket Association of Bengal & Another [1995] 2 SCC 161** for the holding that the right to participate in the affairs of the country is meaningless unless the citizens are well informed on all sides of the issues in respect of which they are called upon to express their views.

586. The 6th Interested Party joined the Petitioners and the 5th Interested Party in faulting the process of enactment of the impugned amendments. It submits that the public had a right to be informed before significant changes were made to the law and given an opportunity to participate publicly in the making of public policies and laws. In addition to the cases already cited by the Petitioners, the 6th Interested Party relied on the case of **Samuel Thinguri Waruathie and 2 Others v Kiambu County Government & 2 Others (2015) eKLR** in support of the principle that public views ought to be considered in the decision-making process and as far as possible, the product of the legislative process ought to be a true reflection of the public participation. It is its submission further, that by using an omnibus Bill to introduce significant changes to the law, the intention was not to enhance and facilitate public awareness and participation but to dilute and circumvent that requirement.

587. It asserts that the Court of Appeal had, in the case of **Law Society of Kenya v The Hon. Attorney General & 2 others, [2019] eKLR**, (hereafter the **2019 Law Society of Kenya Case**) put a seal of approval on the stated law on public participation and the place of omnibus Bills in the passing of laws.

588. The Respondents strenuously oppose the assertion by the Petitioners and the 5th and 6th Interested Parties. They insist that the impugned amendments were passed in compliance with the Constitution. The 1st Respondent submits that there was effective public participation and that the provisions of Article 118 of the Constitution were complied with through publication of the Bill in the local newspapers. Further, that there is no averment that the Petitioners or any other person was denied the opportunity to oversee the process leading to the enactment of the legislation in issue. It is also the 1st Respondent's case that the Petitioners can still invoke the provisions of Article 119 of the Constitution which allows members of the public

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 106 of 205.

to petition Parliament to amend, enact or repeal any legislation, thereby providing another opportunity for public participation.

589. The 1st Respondent submits that public participation was facilitated through the National Assembly's Standing Orders. He relies on the **2013 Law Society of Kenya Case** as affirming the position that the Parliamentary Standing Orders by themselves facilitate public participation in legislative business. The 1st Respondent asserts that the legislature is not bound to enact legislation in accordance with the views of any particular interest group. Further, that public participation should not be used to overrule or veto the acts of the legislature as proposed by the Petitioners. The 1st Respondent relies on the decision in **Kenya Small Scale Farmers Forum & 6 others vs Republic of Kenya & 2 others** (supra) in support of the proposition that the National Assembly has a broad measure of discretion on how it achieves the object of public participation and what matters is that at the end of the day, a reasonable opportunity is offered to members of the public to know about the issues and to have an adequate say.

590. The 1st Respondent further submits, again on the authority of **Kenya Small Scale Farmers Forum & 6 others vs Republic of Kenya & 2 others**, that what amounts to a reasonable opportunity for the public to participate in the enactment of legislation will depend on the circumstances of each case. It is the 1st Respondent's case that the doctrine of public participation was complied with in this case in that on 7th May 2018, advertisements were placed in both the *Standard* and *Daily Nation* newspapers asking for memoranda from stakeholders in respect of the Statute Law (Miscellaneous Amendments) Bill 2018. Further, that the National Assembly Committee on Administration and National Security held stakeholders meetings on 14th, 19th, and 20th June 2018 where the stakeholders, who included the 3rd Petitioner were given an opportunity by the 6th Respondent to present their views on the impugned amendments.

591. In the 1st Respondent's view, not every person must express their views in order to satisfy the constitutional requirement of public participation, citing in support of this argument the **2016 Law Society of Kenya Case**. According to the 1st Respondent, the 3rd Petitioner has not denied the fact that it participated in the process leading to the passing of the impugned amendments, and that of itself is positive proof that public participation was real and not illusory.

592. The 2nd and 3rd Respondents concur with the Petitioners that jurisprudence on the question of public participation in the legislative process requires that the members of the public are given reasonable opportunity to participate in the process. They however contend, relying on decision in **Moses Munyendo & 908 Others vs The Attorney General and Minister for Agriculture** [2013] eKLR, that Parliament has a broad measure of discretion on how it achieves the object of public participation, and that the manner in which public participation is effected varies from case to case.

593. Although the 2nd and 3rd Respondents agree that it must be clear that a reasonable level of participation has been afforded to the public, they argue that what constitutes a reasonable opportunity is incapable of precise definition. They cite the decision of the South African Constitutional Court in the **Doctors for Life Case** for the proposition that the nature and degree of public participation that is reasonable in a given case will depend on the nature and importance of the legislation, and the intensity of its impact on the public. Further, that the

legislature should ensure that the potentially affected section of the population is given a reasonable opportunity to have a say.

594. The 2nd and 3rd Respondents concede that the impugned amendments affect the entire population resident in Kenya. In their view, however, the effect on individual Kenyans is not as radical as submitted by the Petitioners. They contend that the information being sought from Kenyans through NIIMS is substantially the same information as was being sought from them prior to NIIMS. They assert that no substantial amendments were made to the Act in that the impugned amendments merely sought, in digital form, biographical and biometric information that was already registrable under the Act. In support of this assertion they submit that prior to the amendment, section 5(1)(j) of the Act empowered the Registrar to collect such other particulars in addition to the biographical and biometric information expressly outlined in section 5(1) of the Act. It is the 2nd and 3rd Respondents' view therefore, that the Registrar could still have requested for the information now sought under NIIMS based on the law as it existed before the impugned amendments.

595. The 2nd and 3rd Respondents submit that it would not only have been impossible but would also have amounted to imprudent use of resources to expect all Kenyan citizens and foreign nationals residing in Kenya to submit their views on the impugned amendments. It is their position that in any case, reasonable opportunity was provided for those who wished to submit views to do so. The 7th Interested Party is given as an example of an organization which utilized the opportunity for public participation to the maximum. Further, that time was of essence in the enactment of the impugned amendments as it was in the public interest to have a robust, efficient and organized system of identity of persons especially in the wake of terror attacks in the country.

596. The 2nd and 3rd Respondents cite the South African decision in **Land Access Movement of South Africa Association for Rural Development and Others vs Chairperson of the National Council of Provinces and Others**(CCT 40/15) [2016] ZACC 22 in which the court held that the “*standard to be applied in determining whether Parliament has met its obligation of facilitating public participation is one of reasonableness*” and that “*some deference should be paid to what Parliament considered appropriate in the circumstances, as the power to determine how participation in the legislative process will be facilitated rests upon Parliament*”. Further, that the “*Court must have regard to issues like time constraints and potential expense*”.

597. The 2nd and 3rd Respondents rely on the averments by Mr. Michael Sialai, the Clerk to the National Assembly, to stress that not only was public participation conducted, but it was also sufficient. According to the 2nd and 3rd Respondents, the 3rd Petitioner had submitted memoranda in support of the establishment of NIIMS and it cannot now turn around to demonise NIIMS. In their view, this amounts to approbating and reprobating and the 3rd Petitioner should be denied the orders sought on this ground.

598. In their response to the claim by the Petitioners that the enactment of the impugned amendments did not comply with the principle of public participation, the 4th and 7th Respondents submit that public participation was indeed conducted in compliance with the law. They point to the 6th Respondent's response as clearly evidencing the fact that public participation was carried out. They place reliance on the decision in **Josephat Musila Mutua & 9 others v Attorney General & 3 others** [2018] eKLR in support of the assertion that the National Assembly has a broad measure of discretion on how it can achieve the object of

public participation and how public participation is effected will vary from case to case but that it must be clear that a reasonable level of participation was afforded to the public. They also cite the decision in the South African case of **Land Access Movement of South Africa Association for Rural Development and others vs Chairperson of the National Council of Provinces and Others** (supra) as establishing the law on the parameters to be considered in determining whether the standard of public participation was met by the legislature.

599. In response to the contention that the time allowed for public participation was insufficient, the 4th and 7th Respondents justify the sufficiency of the seven days given for members of public to provide their views by referring to the decision in **Simeon Kioko Kithaka & 18 others v County Government of Machakos & 2 others** [2018] eKLR where it was observed that *“even if the period is short but it is shown that the petitioner did in fact participate in the enactment of the Bill, the Court would be reluctant to nullify the enactment in the absence of any evidence that a member of the public was as a result of the short notice locked out from presenting his views.”* They submit that no evidence was adduced by the Petitioners to the effect that a member of the public was locked out from presenting their views. They place reliance for this contention on the averment of Michael Sialai in the supplementary affidavit sworn on 2nd May, 2019 on behalf of the 6th Respondent that stakeholders, including the Petitioners and the Interested Parties supporting the Petitions, were promptly invited for stakeholders’ meetings which were held between 7th May, 2018 and 20th June, 2018. They therefore conclude that there was sufficient public participation.

600. On its part, the 5th Respondent submits that contrary to the claim by the Petitioners, the doctrine of public participation was complied with in the enactment of the impugned amendments. The **Robert Gakuru Case** and **Doctors for Life Case** as well as **Minister of Health and Another v New Clicks South Africa (Pty) Ltd and Others**(2006) (2) SA 311 (CC); **Land Access Movement of South Africa Association for Rural Development and others v Chairperson of the National Council of Provinces and others** (supra) ; **Ngige Tharau & 128 Others v Principal Secretary of Lands, Housing and Urban Development & 2 others**[2016] eKLR; **Diani Business Welfare Association and Others v The County Government Of Kwale** [2015] eKLR; and **Nairobi Metropolitan PSV Saccos Union Ltd & 25 Others v County Government of Nairobi & 3 Others** [2014] eKLR are cited as espousing the law on public participation.

601. The 5th Respondent agrees with the other Respondents that the invitation for comments on the Statute (Miscellaneous Amendment) Bill 2018 published in the *Standard* and *Daily Nation* newspapers is evidence of public participation. He further argues that oral and written comments were received from various state agencies and the affected stakeholders. On that basis, the 5th Respondent urges the Court to hold that reasonable opportunity was granted to the members of the public to have a say on the impugned amendments.

602. The 6th Respondent, not surprisingly, submits passionately on the issue of the alleged unconstitutionality of the impugned amendments. He starts by highlighting the principles for constitutional interpretation, noting, *inter alia*, that in considering the constitutionality of an Act or a provision thereof, the rebuttable principle of presumption of constitutionality of statutes should be taken into account. He further submits that the principle which states that statutes should be presumed to be constitutional until the contrary is proved is founded on the philosophy that Parliamentarians, as peoples’ representatives, legislate laws to serve the people they represent and therefore, as legislators, they understand the problems people face and enact laws to solve the problems. It is further the 6th Respondent’s case that Article

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 109 of 205.

186(4) of the Constitution gives powers to Parliament to legislate on any matter for the Republic of Kenya.

603. While referring to the facts of the case and the contents of the replying affidavit by Mr. Michael Sialai, the Clerk of the National Assembly, the 6th Respondent submits that the evidence clearly reveals that the impugned amendments were enacted in accordance with the Constitution. Accordingly, the impugned sections of the Act are constitutional. The 6th Respondent points to the contents of the replying affidavit which he submits detail the procedure used in passing the impugned amendments and which confirms full compliance with the Constitution.

604. The 6th Respondent stresses the legislative autonomy of the National Assembly by citing Articles 94 and 109 of the Constitution. It is his case that the two houses of Parliament can exercise their legislative will by enacting laws and amending existing laws as well as Bills which are before them. He states that it was in exercise of that power that the National Assembly debated and passed the Statute Law (Miscellaneous Amendments) Bill (National Assembly Bill No. 12 of 2018) and the President assented to the Bill to become law.

605. With respect to the assertion by the Petitioners that there was no compliance with the principle of public participation in the enactment of the impugned amendments, the 6th Respondent submits that the National Assembly conducted public participation and took the views of the public into account as evidenced by the replying affidavit of Mr. Michael Sialai. He cites the decision in the **Robert Gakuru Case** as stating the law on the principle of public participation and points out that the said decision was upheld by the Court of Appeal. It is his submission that the decisions in the **Robert Gakuru Case** and the **2016 Law Society Case** confirm the principle that not all persons must express their views on the proposed legislation in order for the principle of public participation to be satisfied.

606. The 6th Respondent maintains that the requirement for public participation was met. He points out that during the process of the enactment of the Statute Law (Miscellaneous Amendment), 2018 each National Assembly Departmental Committee was tasked to examine each amendment as if they were distinct legislations. He further argues that in the advertisement calling for submission of comments, each thematic area was distinctively before a relevant departmental committee as per the Second Schedule of the National Assembly Standing Orders. It is also his submission that in the newspaper advertisements, the committee to deal with each subject matter was indicated hence giving guidance to the public on where to make representations.

607. The 6th Respondent, reiterates in his submissions the averments by Mr. Sialai that each proposed amendment was treated separately since, during debates on the Bill, the Chairpersons of the respective committees were given time to indicate views of the committees and the public; that unlike in the past where all the amendments were moved by the Chairman of the Justice and Legal Affairs Committee, in this instance, the Chairpersons of the relevant committees moved their respective amendments. It is his submission that these were deliberate adjustments of the rules of procedure to accommodate examination of the amendments by the House.

608. In its submissions, the 1st Interested Party agrees with the Respondents that the legislative process of the impugned amendments was not attended by any constitutional infirmity. On the issue of public participation, its submission is that the 6th Respondent's affidavits particularly demonstrate beyond any shadow of doubt that advertisements were

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 110 of 205.

placed in the print media inviting members of the public to submit memoranda on the Bill that culminated in the enactment of the impugned amendments.

609. The 1st Interested Party urges the court to give space to Parliament to discharge its constitutional mandate. It cites in support of this argument the South African case of **Land Access Movement of South Africa Association for Rural Development and others v Chairperson of the National Council of Provinces and others** (supra) in which it was observed that when determining the question whether Parliament's conduct was reasonable, some deference should be paid to what Parliament considered appropriate in the circumstances. This is on the basis that the power to determine how participation in the legislative process will be facilitated rests upon Parliament. The 1st Interested Party also relies on **The 2016 Law Society Case** in which it was stated that with regard to public participation, the court has to look at the entire process and Parliamentary Standing Orders. The 1st Interested Party concludes that the Petitioners have not demonstrated that the law was not followed in the enactment of the impugned amendments and calls for the dismissal of the Petitions.

610. We have considered the respective submissions of the parties on the question whether the principle of public participation was complied with in the enactment of the impugned amendments. We observe at the outset that the need to involve the public in the legislative processes is grounded in the Constitution.

611. The national values and principles of governance set out in Article 10(2) of the Constitution include democracy and participation of the people, good governance, transparency and accountability. Participation of the people in governance is therefore a constitutional imperative. In reference to the legislative process, the concept of public participation is cemented by Article 118(1) which requires Parliament to conduct its business in an open manner. Its sittings and those of its committees are to be opened to the public. Apart from the requirement for transparency, the Constitution directs Parliament and its committees to facilitate public participation and involvement in its legislative processes and other businesses.

612. The principle of public participation is recognized internationally. In the **Doctors for Life Case**, Ngcobo, J. observed that this principle is embedded in international and regional human rights instruments. The doctrine encompasses the right to participate in political affairs as well as the indirect participation through elected representatives. There is also the general right to directly take part in the conduct of public affairs. The latter is the aspect of the principle of public participation that is of concern to us in this matter.

613. In the **Doctors for Life Case**, Ngcobo, J highlighted the ingredients of the right of the public to participate in governance affairs and the measures to be taken in order to fulfill this obligation. He stated that:

“The general right to participate in the conduct of public affairs includes engaging in public debate and dialogue with elected representatives at public hearings. But that is not all; it includes the duty to facilitate public participation in the conduct of public affairs by ensuring that citizens have the necessary information and effective opportunity to exercise the right to political participation.... Thus construed, there are at least two aspects of the duty to facilitate public involvement. The first is the duty to provide meaningful opportunities for public participation in the law-making process.

The second is the duty to take measures to ensure that people have the ability to take advantage of the opportunities provided. In this sense, public involvement may be seen as “a continuum that ranges from providing information and building awareness, to partnering in decision-making.” This construction of the duty to facilitate public involvement is not only consistent with our participatory democracy, but it is consistent with the international law right to political participation. As pointed out, that right not only guarantees the positive right to participate in the public affairs, but it simultaneously imposes a duty on the State to facilitate public participation in the conduct of public affairs by ensuring that this right can be realised.”

614. The Learned Judge went on to identify the fruits of participatory democracy by stating that:

“The participation by the public on a continuous basis provides vitality to the functioning of representative democracy. It encourages citizens of the country to be actively involved in public affairs, identify themselves with the institutions of government and become familiar with the laws as they are made. It enhances the civic dignity of those who participate by enabling their voices to be heard and taken account of. It promotes a spirit of democratic and pluralistic accommodation calculated to produce laws that are likely to be widely accepted and effective in practice. It strengthens the legitimacy of legislation in the eyes of the people. Finally, because of its open and public character it acts as a counterweight to secret lobbying and influence peddling. Participatory democracy is of special importance to those who are relatively disempowered in a country like ours where great disparities of wealth and influence exist. Therefore our democracy includes as one of its basic and fundamental principles, the principle of participatory democracy. The democratic government that is contemplated is partly representative and partly participatory, is accountable, responsive and transparent and makes provision for public participation in the lawmaking processes”.

615. Although Ngcobo, J acknowledged that the law requires the involvement and the facilitation of the public in public affairs, he was of the view that the manner and means of achieving public participation in the legislative processes should be left to Parliament. In that regard, he held that:-

“Parliament and the provincial legislatures must be given a significant measure of discretion in determining how best to fulfil their duty to facilitate public involvement. This discretion will apply both in relation to the standard rules promulgated for public participation and the particular modalities appropriate for specific legislative programmes. Yet however great the leeway given to the legislature, the courts can, and in appropriate cases will, determine whether there has been the degree of public involvement that is required by the Constitution. What is required by section 72(1)(a) will no doubt vary from case to case. In all events, however, the NCOP must act reasonably in carrying out its duty to facilitate public involvement in its processes”.

616. The fact that non-compliance with the principle of public participation can result in the declaration of a law invalid was confirmed by Ngcobo J when he held that:

“When legislation is challenged on the grounds that Parliament did not adopt it in accordance with the provisions of the Constitution, courts have to consider whether in enacting the law in question Parliament has given effect to its constitutional obligations. If it should hold in any given case that Parliament has failed to do so, it is obliged by the Constitution to say so. And insofar as this constitutes an intrusion into the domain of the legislative branch of government, that is an intrusion mandated by the Constitution itself. What should be made clear is that when it is appropriate to do so, courts may – and if need be must – use their powers to make orders that affect the legislative process. Therefore, while the doctrine of separation of powers is an important one in our constitutional democracy, it cannot be used to avoid the obligation of a court to prevent the violation of the Constitution.”

617. As to what the court should consider in determining whether the constitutional standards of public participation were met in the enactment of a given legislation, Ngcobo, J identified some of the factors to be taken into account as follows:-

“Whether a legislature has acted reasonably in discharging its duty to facilitate public involvement will depend on a number of factors. The nature and importance of the legislation and the intensity of its impact on the public are especially relevant. Reasonableness also requires that appropriate account be paid to practicalities such as time and expense, which relate to the efficiency of the law-making process. Yet the saving of money and time in itself does not justify inadequate opportunities for public involvement. In addition, in evaluating the reasonableness of Parliament’s conduct, this Court will have regard to what Parliament itself considered to be appropriate public involvement in the light of the legislation’s content, importance and urgency. Indeed, this Court will pay particular attention to what Parliament considers to be appropriate public involvement. What is ultimately important is that the legislature has taken steps to afford the public a reasonable opportunity to participate effectively in the law-making process.”

618. It is not incorrect to state that the development of the law on public participation in the legislative process is advanced in our jurisdiction. There are quite a number of decisions in this area. Odunga, J. did comprehensive work on the issue in his decision in the **Robert Gakuru Case**. The learned Judge extensively reviewed the jurisprudence relating to the principle of public participation and reached the conclusion that:-

“In my view public participation ought to be real and not illusory and ought not to be treated as a mere formality for the purposes of fulfilment of the Constitutional dictates. It is my view that it behoves the County Assemblies in enacting legislation to ensure that the spirit of public participation is attained both quantitatively and qualitatively. It is not just enough in my view to simply “tweet” messages as it were and leave it to those who care to scavenge for it. The County Assemblies ought to do whatever is reasonable to ensure that as many of their constituents in particular and the Kenyans in

general are aware of the intention to pass legislation and where the legislation in question involves such important aspect as payment of taxes and levies, the duty is even more onerous. I hold that it is the duty of the County Assembly in such circumstances to exhort its constituents to participate in the process of the enactment of such legislation by making use of as may (sic) fora as possible such as churches, mosques, temples, public barazas national and vernacular radio broadcasting stations and other avenues where the public are known to converge to disseminate information with respect to the intended action”.

619. In the **2019 Law Society Case** the Court of Appeal stressed the place of the principle of public participation in governance by stating that:

“From the finding above, the learned judge ought to have found in favour of the appellant based on the claim made on the lack of public participation. It was an error for the learned judge to require the appellant to prove the negative, for once it states there was no public participation, the burden shifted to the respondents to show that there was. Much weight has been placed on public participation because it is the only way to ensure that the Legislature will make laws that are beneficial to the mwananchi, not those that adversely affect them.

Additionally, the onus is on Parliament to take the initiative to make appropriate consultations with the affected people. It is therefore a misdirection for the learned judge to hold that the appellant had the responsibility to prove that the consultations did not happen. We believe that the principle behind the amendments is what must be interrogated. The 1st respondent is not possessed of an unfettered or carte blanche leeway to table legislation that is detrimental to the people of Kenya or a section of the citizenry. It must follow due process which includes consultation with stakeholders. The Constitution establishes that mechanism to enable the Legislature make laws that are reasonable, having sought and obtained the views of the people. That is the essence of an accountable limited Government and the shift from the supremacy of Parliament to the Sovereignty of the people birthed by the 2010 Constitution.”

620. The principle of public participation does not require the legislature to conduct a census-like exercise of knocking at the door of every person residing in its jurisdiction with a view to confirming that the residents have given their opinions on a contemplated legislative measure, and where no comments are forthcoming, to ‘forcefully’ extract opinions from residents. The duty placed upon the legislature by the law is to inform the public of its business and provide an environment and opportunity for those who wish to have a say on the issue to do so. Indeed in the case of **Kiambu County Government & 3 others v Robert N. Gakuru & Others** [2017] eKLR, the Court of Appeal aptly summarized the principle of public participation thus:-

“The bottom line is that public participation must include and be seen to include the dissemination of information, invitation to participate in the process and consultation on the legislation.”

621. Public participation requires that the legislature takes into consideration the views expressed by the public. The importance of taking into consideration the views received from the public in the legislative process was affirmed by Sachs, J in the South African case of **Merafong Demarcation Forum and Others v President of the Republic of South Africa and Others** (CCT 41/07) [2008] ZACC 10; 2008 (5) SA 171 (CC); 2008 (10) BCLR 968 (CC) when he stated that:-

“The passages from the Doctors for Life majority judgment, referred to by the applicants, state reasons for constitutionally obliging legislatures to facilitate public involvement. But being involved does not mean that one’s views must necessarily prevail. There is no authority for the proposition that the views expressed by the public are binding on the legislature if they are in direct conflict with the policies of Government. Government certainly can be expected to be responsive to the needs and wishes of minorities or interest groups, but our constitutional system of government would not be able to function if the legislature were bound by these views. The public participation in the legislative process, which the Constitution envisages, is supposed to supplement and enhance the democratic nature of general elections and majority rule, not to conflict with or even overrule or veto them. To say that the views expressed during a process of public participation are not binding when they conflict with Government’s mandate from the national electorate, is not the same as cynically stating that the legislature is not required to keep an open mind when engaging in a process of that kind. Public involvement cannot be meaningful in the absence of a willingness to consider all views expressed by the public.”

622. As emerges from the submissions above, all the parties agree that public participation is a key element in the achievement of democratic governance and is a constitutional imperative. All the parties also agree that the 3rd Respondent invited memoranda from the public through adverts in the *Standard* and *Daily Nation* newspapers of 7th May, 2018. According to the Respondents and the Interested Parties opposing the Petition, the advertisement fulfilled the constitutional requirement for public participation. The Petitioners and the Interested Parties who support the Petition think otherwise. The issue for determination therefore revolves around the sufficiency or otherwise of the public participation conducted in respect of the impugned amendments.

623. In **Mui Coal Basin Local Community & 15 Others** (*supra*) the Court expressed itself on the question of threshold of public participation as follows:

“92. The main question in this context then becomes, what is the test for determining if the threshold of public participation has been met” We are aware that several Courts in Kenya have dealt with the issue. The emerging position in Kenya is exemplified by the decision and reasoning of Justice Emukule in John Muraya Mwangi & 495 Others & 6 Others V Minister For State For Provincial Administration & Internal Security & 4 Others [2014 eKLR. Since it demonstrates the emerging consensus, we apologise for quoting at length the reasoning of the Learned Judge thus:

“The concept of public participation enshrined in Articles 10 and 12 of the Constitution of Kenya 2010, is a difficult one but needs to be given effect both before and after legislative enactment. This may take several forms:-

- i. The concept envisages political participation in the conduct of public affairs, such as the right to vote, and to be elected or appointed to public office,***
- ii. The right to be engaged in public debate and dialogue with elected representatives at public hearings,***
- iii. The duty to facilitate public participation in the conduct of public affairs,***
- i. Ensuring that ordinary citizens the “hoi polloi,” the “lala hoi” have the necessary information and are given opportunity to exercise their say not merely in election and appointment to political office but also economic participation, and conduct of their affairs.”***

624. As to how to determine whether the public participation conducted was sufficient, the Court stated that:

“96. The issue then arises of how we measure what is sufficient. In our determination we agree with the test applied in the Merafong Demarcation case and state that, the method and degree of public participation that is reasonable in a given case depends on a number of factors, including the nature and importance of the issue at hand and the intensity of its impact on the public.”

625. Even though the cited principles are couched in the context of the day to day governance of the populace, we find them applicable to some extent to execution of legislative business by Parliament.

626. Through Standing Order No. 127 of the National Assembly Standing Orders (4th Edition), the National Assembly incorporates the constitutional principle of public participation in its legislative business by providing that:

“127. (1) A Bill having been read a First Time shall stand committed to the relevant Departmental Committee without question put.

(2)

(3) The Departmental Committee to which a Bill is committed shall facilitate public participation on the Bill through appropriate mechanism, including-

- (a) inviting submission of memoranda;***
- (b) holding public hearings;***
- (c) consulting relevant stakeholders in a sector; and***
- (d) consulting experts on technical subjects.***

(3A) The Departmental Committee shall take into account the views and recommendations of the public under paragraph (3) in its report to the House.”

627. We find that the said provision does indeed incorporate the principles of public participation. A close reading of the provision readily discloses that Parliament has the discretion on the method to be used in collecting views from the public, stakeholders and experts. This observation is in line with the case law on public participation.

628. In the **Doctors for Life** case Ngcobo, J was of the opinion that:

“Whether a legislature has acted reasonably in discharging its duty to facilitate public involvement will depend on a number of factors. The nature and importance of the legislation and the intensity of its impact on the public are especially relevant. Reasonableness also requires that appropriate account be paid to practicalities such as time and expense, which relate to the efficiency of the law-making process. Yet the saving of money and time in itself does not justify inadequate opportunities for public involvement. In addition, in evaluating the reasonableness of Parliament’s conduct, this Court will have regard to what Parliament itself considered to be appropriate public involvement in the light of the legislation’s content, importance and urgency. Indeed, this Court will pay particular attention to what Parliament considers to be appropriate public involvement. What is ultimately important is that the legislature has taken steps to afford the public a reasonable opportunity to participate effectively in the law-making process.”

629. The Petitioners and the Interested Parties who support them have decried the lack of information in regard to the impugned amendments and NIIMS itself. They also raise the issue of the sufficiency of time given to the public to submit their views. The request for representations from the public was published in the newspapers on 7th May, 2018, and the representations were to be submitted before the close of business on 14th May, 2018. The Respondents and the Interested Parties aligned to their cause insist that the pre-enactment information on the impugned amendments and the post-enactment education on NIIMS was sufficient in the circumstances of this case.

630. We note that neither of the parties addressed us on which party bears the responsibility of informing the public on the Bills for purposes of public participation in the legislative process. This is in light of the fact that the legislative process begins from policy formulation stage, and the sponsor of a legislation, who has the background information, is a different entity from Parliament. Therefore, placing the onus on Parliament alone in this respect may be impracticable and unreasonable. In addition, there are opportunities to engage citizens at various stages of the legislative process, and these can be coordinated by various actors who are responsible for the process at any given stage, including during the content development of a Bill. Accordingly, there are roles to be played by the Executive, civil society and Parliament in education the public as actors in the various stages of the development of a Bill.

631. Be that as it may, we note that the 6th Respondent annexed a copy of the Statute Law (Miscellaneous Amendments Bill) 2018 together with a Memorandum of Objects and Reasons to its Replying Affidavit sworn on 28th February 2019 by Michael Sialai. The said Memorandum of Objects and Reasons explained that the Bill proposed to amend the Registration of Persons Act to establish the National Integrated Identity Management System, Petition 56, 58 & 59 of 2019 (Consolidated) | Page 117 of 205.

and provide for the capture of biometric data and geographical data in the registration of persons in Kenya. The said Bill was published in the Kenya Gazette Supplement No. 35 (National Assembly Bills No 12) on 10th April 2018. In terms of the legislative process, the Bill and Memorandum of Reasons and Objects was therefore in the public domain from 10th April 2018.

632. The 6th Respondent also annexed a copy of the advertisement in the *Daily Nation* newspaper of 7th May 2018. The said advertisement informed the public about three events. Firstly, on the publication of the Bill on 10th April 2018. Secondly, that the amendments in the Bill to the various Acts would be committed to various Departmental Committees of the National Assembly that were listed in the advertisement. Lastly, of an invitation to members of the public to submit any representations they may have on the Bill. In this respect, the amendments to the Registration of Persons Act were shown to be committed to the Administration and National Security Committee of the National Assembly. The minutes of the sittings of the said Committee on 14th, 19th, and 20th June 2019 when the amendments were discussed were also annexed, as was a copy of a memorandum sent by the 3rd Petitioner dated 25th May 2018 on the said amendments.

633. The Petitioners on the other hand rely on the advertisement published on 7th May 2018 to show that there was insufficient time for public participation, and the contents of the Bill, which was amending 68 Acts of Parliament.

634. Our view is that the time that was available for public participation must be considered in light of all the processes of the legislative process. In the present Petition, the evidence before us suggests that the public was aware of the Bill from 10th April 2018, when it was published, and could have participated from that date. The purpose of publication of Bill in this regard is to notify the public and invite representations through the elected Members or direct submission of memoranda and petitions. It is therefore not entirely correct to state that the members only had the seven days indicated in the advertisement of 7th May 2018 to present their views on the Bill. Even after expiry of the seven days, the doors were not closed for members of the public to participate, as there was still opportunity to participate during the committee hearings as shown in Standing Order 127. The evidence from the Respondent demonstrates that this opportunity was availed, and that indeed there was participation by the 3rd Petitioner even after expiry of the time stated in the advertisement. It is thus our finding that sufficient time was availed for public participation on the enactment Statute Law (Miscellaneous Amendments Bill) 2018.

635. There is sufficient authority for the proposition that the entire process has to be interrogated in order to determine whether the requirement for public participation was fulfilled in respect of a given law. In **2013 Law Society Case** the Court held that:

“In order to determine whether there has been public participation, the court is required to interrogate the entire process leading to the enactment of the legislation; from the formulation of the legislation to the process of enactment of the statute.”

636. We also recognize that there were efforts made by the National Assembly in facilitating public participation when using the omnibus Bill mechanism in the Statute Law (Miscellaneous Amendments) Bill 2018. Unlike in the case of **2013 Law Society Case** where the object of the Bill was clearly indicated as intended to effect minor amendments, in the instant case there was clear indication that the legislature intended to carry amendments on Petition 56, 58 & 59 of 2019 (Consolidated) | Page 118 of 205.

the targeted Acts without the use of the term ‘minor’. It is also clear that from the advertisement of 7th May 2018 that each Act targeted for amendment was linked to the relevant committee. Therefore, in effect, only a part of the amendments and not all of them were subject to stakeholder engagement in the Committees. Coupled with the fact that there was sufficient time availed to the public to give their views on the amendments, we find that there was sufficient public participations in the circumstances of these Petitions.

The Use of an Omnibus Bill to Effect the Impugned Amendments

637. The second aspect of the Petitioners’ challenge to the impugned amendments is that it was effected by way of an omnibus miscellaneous statute. In this regard, the 1st Petitioner submits that the violation of the Constitution can occur either through form or content. Its view is that whether the violation is one of form or content, any violation is sufficient for the court to find that an impugned law is unconstitutional. The position taken by the 1st Petitioner is that the impugned amendments were substantive since they were fashioned to overhaul the manner in which registration and identification of Kenyans and foreign nationals is done. They also created a new system of registration and storage of the data. The 1st Petitioner identified the various laws affected by the amendments to demonstrate the far-reaching effects of the changes.

638. Additionally, the 1st Petitioner submits that the implementation of NIIMS affects, in different ways, other aspects regulated by other laws, for example the Children Act, Prevention of Terrorism Act and the National Police Service Act. Moreover, the infrastructural outlay required to implement it is enormous and it further affects many other areas of both national and county governments’ competencies, including provision of services such as health, education and housing. The 1st Petitioner contends that the implementation of NIIMS affects significant aspects of public administration and straddles areas of constitutional competencies of both national and county governments and at least in part, it seeks to implement the 2017 Nouakchott Declaration of the African Union on digitization.

639. In light of these submissions, the 1st Petitioner contends that the use of the miscellaneous amendment process was inappropriate considering that the courts have limited the use of the process for minor and non-controversial amendments. Reliance is placed on the decision in the **2016 Law Society Case** where it was held that omnibus amendments in the form of statute law miscellaneous legislations ought to be confined only to minor non-controversial and generally house-keeping amendments.

640. The 1st Petitioner’s position is that the empowerment of the Respondents by the law to collect sensitive personal information such as DNA and GPS coordinates can neither be minor nor non-controversial. Moreover, the major amendments to the Act involve spending of significant amounts of public funds, involve the introduction of a new registration body and processes, and will prejudicially affect the rights of persons. Such amendments, in the 1st Petitioner’s view, ought not to have been done through a miscellaneous amendment. It is therefore the 1st Petitioner’s submission that the use of miscellaneous amendment process to effect significant amendments to the Act is unconstitutional and to that extent, the amendments are null and void.

641. The 2nd Petitioner supports the position taken by the 1st Petitioner on the use of an omnibus law. It also places reliance on the **2016 Law Society Case** for the proposition that the use of the omnibus procedure in the enactment of laws ought to be confined only to minor non-controversial and generally house-keeping amendments. It asserts that the impugned

amendments have far-reaching implications on fundamental rights and freedoms protected under the Bill of Rights. In the 2nd Petitioner's opinion, the impugned amendments not only deserved robust input from the public but were also deserving of better and intense debate and deliberations by the National Assembly and the Senate to ensure proper consideration of all the concerns.

642. The 2nd Petitioner contends that embedding the impugned amendments in an omnibus Bill containing amendments of 67 other statutes unnecessarily rushed their passage with the obvious consequence that the public and Parliament itself were deprived of the opportunity to exhaustively debate the reasonableness and necessity of the amendments relative to their stated objective. Further, that if the proceedings of the relevant Departmental Committee and the Whole House are anything to go by, it is *ex facie* evident that in spite of their apparent implications on fundamental rights and freedoms and particularly the right to privacy, the full import of the amendments was not at all debated and the logical inference from this is that either the legislators did not appreciate the extensive consequences of the amendments or they had no reasonable opportunity to debate them, as they would have done, had the impugned amendments been presented as a stand-alone Bill. In the 2nd Petitioner's view, the enactment of the impugned amendments amounted to abuse of legislative discretion and a breach of public trust.

643. The 3rd Petitioner joined the 1st and 2nd Petitioners in faulting the National Assembly for using an omnibus Bill to pass the impugned amendments. It is the 3rd Petitioner's submission that statutory amendments by way of statute law miscellaneous legislation should strictly be confined to cases of minor non-controversial amendments as was held in the **2019 Law Society Case**. Its view is that the impugned amendments breached the said legal principle in that the amendments were substantial and should not have been introduced through a Miscellaneous Amendment Act.

644. The 5th Interested Party also agrees with the position taken by the Petitioners and the authorities relied on in support of the contention that omnibus amendments in the form of Statute Law Miscellaneous legislation ought to be confined only to minor non-controversial and generally house-keeping amendments. It further cites the case of **Okiya Omtatah v The Communication Authority of Kenya & 21 others** [2017] eKLR for the proposition that an omnibus Bill is designed to make only relatively minor, non-controversial amendments to various Acts and to repeal Acts that are no longer required and assist in expediting the government's legislative programme and Parliamentary business by reducing the number of separate amendment Bills that deal with relatively minor amendments and repeals. Further, that an amendment that has an impact on either the letter or the spirit of the Constitution, however remotely, cannot be termed a minor, non-controversial house-keeping amendments. The 5th Interested Party therefore submits that NIIMS squarely falls outside the confines of the province of '*minor non-controversial and generally house-keeping amendments*' and ought not to have been passed as a miscellaneous amendment.

645. The 5th Interested Party identifies the large amount of public funds spent in the creation of NIIMS as another facet of the defects in the procedure used in the enactment of the legislation establishing it. It also relies on the **2016 Law Society Case** in which the Court relied on the Canadian Miscellaneous Statute Law Amendment Program to hold that for a Bill to qualify as non-controversial, it should not involve the spending of public funds, prejudicially affect the rights of persons, or create new offences or subject a new class of persons to an existing offence. It is the 5th Interested Party's case that the Respondents are on

record as admitting expenditure of public funds on the project. It submits that for the above reasons, it was improper to introduce NIIMS through a Statute Law (Miscellaneous) Amendment Bill. The 5th Interested Party therefore asks the court to find that the amendments were unlawful and unconstitutional.

646. The 6th Interested Party agrees with the Petitioners on the unconstitutionality of the impugned amendments. It asserts that the very use of an omnibus Statute Law Miscellaneous Amendment Act betrayed the mischief on the part of the Respondents, which was to defeat the public's right and interest to examine the legislation and participate in public affairs and governance. In its view, the object and scope of a Statute Law Miscellaneous Amendment Act is to correct anomalies, inconsistencies, outdated terminology or errors, which are minor, non-controversial amendments to a number of statutes using a single Bill.

647. According to the 6th Interested Party, the impugned amendments were *prima facie* not minor or non-controversial as they did not seek to correct anomalies, inconsistencies or outdated terminology or errors but instead brought about significant changes to the law and introduced wholly new concepts. To buttress this argument, the decision in the **2016 Law Society Case** is identified as explaining the circumstances under which statutory amendments can be made by use of Statute Law Miscellaneous legislation. It is its submission that the five-judge bench which heard the matter looked at the position in various countries and ultimately concluded that while there is no internationally accepted position on the legality of omnibus Bills, both on policy and good governance, omnibus amendments in the form of Statute Law Miscellaneous legislations ought to be confined only to minor non-controversial and generally house-keeping amendments.

648. On the authority of the case of **Josephat Musila Mutua & 9 Others v Attorney General & 3 Others (2018) eKLR** the 6th Interested Party contends that provisions that affect fundamental rights and freedoms are substantial amendments. It submits that the introduction of the new markers or identifiers into the Act were not minor or insignificant amendments but were significant changes with serious import on the fundamental rights and freedoms of Kenyans, clawing back on the autonomy of Kenyans and the right to be informed and to have a say on such significant matters of constitutional significance.

649. The Respondents counter the arguments by the Petitioners and Interested Parties who support them by arguing that there is no constitutionally prescribed procedure for amendment of any statute. According to the 1st Respondent, the Constitution envisages that it is the legislature that will formulate the procedure for enactment of legislation, provided the procedure facilitates public participation and public access as required under Articles 118 and 124 of the Constitution. Further, that legislative procedure and policy are exclusively within the ambit of the legislature under the doctrine of separation of powers and the court and any other arm of government ought not to question the wisdom of Parliament in preferring one procedure over another provided such procedures are facilitative of public participation and access. The 1st Respondent takes the view that global jurisprudence on when and how omnibus Bills can be used is contradictory.

650. As regards the procedural propriety of the enactment of the impugned amendments, the 2nd and 3rd Respondents submit that the law was complied with. They contend that Article 124 of the Constitution allows the National Assembly to establish its own procedures for the conduct of its proceedings. Further, that Article 109 vests in Parliament absolute power to exercise legislative powers through Bills. It is their case that pursuant to the practice of the

National Assembly, a Miscellaneous Amendment Bill connotes a Bill that amends various legislations. They state that the Bill in contention was indeed titled “*A Bill for an Act of Parliament to make various amendments to statute law*,” and was not described by the phrase “*minor amendments*”. More importantly, that during the enactment of the Bill, each Departmental Committee examined respective clauses of relevance to their dockets as if they were distinct legislations. That in particular, Clause 9, which forms the subject matter of these proceedings was examined by the National Assembly Committee on Administration and National Security. The 2nd and 3rd Respondents observe that during the debates on the Bill, the chairpersons of the respective committees were given an opportunity to submit the views of their respective committees and the public.

651. It is the 2nd and 3rd Respondents’ further argument that as was held by the Supreme Court in its advisory opinion in the case of **Speaker of the Senate & another v Attorney-General & 4 others [2013] eKLR**, courts should not supervise the workings of Parliament. They therefore urge the court to allow Parliament to regulate its internal matters as affirmed by the Supreme Court. Further, that it cannot be argued that the usage of a Statute Law (Miscellaneous Amendments) Bill militated against effective public participation for the simple reason that the National Assembly took steps to ensure that the quality of public participation was not compromised.

652. On their part, the 4th and 7th Respondents submits that the Petitioners’ allegation that introducing substantive amendments through omnibus means is unconstitutional lacks any constitutional foundation. Their case is that the Petitioners have failed to set out with a degree of precision the constitutional provision alleged to have been infringed. In their view, in the absence of a claim that the legislation passed by the legislature or the process by which the legislation was enacted violates the Constitution, any consideration of the matter by this Court would amount to unconstitutional intrusion on Parliament’s legislative mandate and a violation of the doctrine of separation of powers. This averment is supported by the decision in **United States v Butler, 297 U.S. 1[1936]**.

653. In response to the Petitioners’ allegation that the omnibus Bill inhibited public participation hence violated Articles 10(2)(a) and 118(1)(b) of the Constitution, the 4th and 7th Respondents submit that no evidence was tendered before this Court to demonstrate that due to the nature, form and structure of the Statute Laws (Miscellaneous Amendments) Act No. 18 of 2018), a member of the public was prevented from presenting their views to Parliament. They therefore urge the Court to hesitate to supervise the manner in which Parliament executes its legislative mandate in the absence of a link between the impugned amendments and a specific constitutional or statutory provision that has been violated or is threatened with violation.

654. It is the 4th and 7th Respondents’ submission that the effectiveness of the legislative mechanism of omnibus Bills must be considered against the importance of the principle of the separation of powers and the principles of representative democracy. In support of this assertion, they cite the decision of the Supreme Court of Israel in **Israel Poultry Farmers Association v. Government of Israel HCJ 4885/03 at 383** where it was held that not every formal defect in the legislative process and not every case of *ultra vires* would lead to intervention in the legislative process by the court. Further, that for the law to be invalidated, it is not sufficient to prove a violation of a basic principle of the legislative process, such as the principle of participation, but it is also necessary to show a severe and substantial violation of that principle.

655. The 4th and 7th Respondents' assertion that there was nothing wrong in the use of an omnibus Bill to effect the impugned amendments was boosted by a reference to the doctrine of separation of powers. It is the 4th and 7th Respondents' contention that the doctrine of separation of powers is not alien to our jurisprudence as was stated by the Court of Appeal in **Mumo Matemu v Trusted Society of Human Rights Alliance & 5 Others C. A. No. 290 of 2012**. They contend that though the arms of government are co-dependent, each branch is reasonably expected to perform its constitutional functions in the best interest of the people on whom sovereign power lies. In doing so, it is presumed that the decisions taken by each branch of government are legitimate and rational, until the contrary is proven. The decision in the case of **Community Advocacy and Awareness Trust & 8 others v Attorney General & 6 others [2012] eKLR** is relied on in support of the proposition that courts must resist the temptation to second-guess the legislature or act as a super legislature and review every piece of legislation. The 4th and 7th Respondents stress that by dint of Article 94 (1) as read with Article 94(5) of the Constitution, legislative authority is exclusively vested in Parliament and no other person or body has the power to make provisions having the force of law in Kenya.

656. The 4th and 7th Respondents conclude by submitting that nowhere in the Constitution or the Standing Orders of the National Assembly is it prescribed that a Bill should contain a single subject; what is referred to as the 'single subject rule' provision. It is their submission that unlike in the United States of America where 43 States have the '*single subject provision*', Kenya has no such provision and it would amount to an infraction of the legislative prerogative of Parliament to arrive at the Petitioners' desired outcome by reading non-existent provisions into the Constitution. It is their case that the Petitioners' allegation that omnibus Bills infringe Articles 10, 73, 93(2) and 94(4) is therefore unfounded. In their view, the cited provisions espouse the constitutional principles that bind Parliament in the discharge of its legislative mandate and nothing more. Further, that the Petitioners had failed to adduce cogent evidence to demonstrate the manner in which the Respondents had violated the Constitution and the specific Article violated.

657. The 5th Respondent did not make any comments on the use of an omnibus Bill to enact the impugned amendments. In support of his position that the impugned amendments were not unconstitutional for having been passed by way of an omnibus Bill, the 6th Respondent argues that a Miscellaneous Amendment Bill amends various legislations and the long title of the Bill usually states the intention and purpose of the Bill. He notes that the long title for the Statute Law (Miscellaneous Amendment) Bill 2018 was "*A Bill for An Act of Parliament to make various amendments to statute law*", and, unlike the Statute Law (Miscellaneous Amendment) Bills for 2015 and 2016 whose long titles were "*A Bill for An Act of Parliament to make minor amendments to statute law*", the word '*minor*' was not used in the 2018 statute. He asserts that neither the Constitution nor the rules of the National Assembly disallow the use of miscellaneous amendment Bills.

658. Developing his case from the above assertions, the 6th Respondent argues that Article 124 of the Constitution gives the National Assembly power to establish Standing Orders to regulate conduct of Parliamentary proceedings. He submits that Article 109 of the Constitution gives absolute power to Parliament to exercise legislative authority which is derived from the people. The implication of this, in the 6th Respondent's view, is that the Constitution has not defined and or limited the legislative processes and powers of Parliament and it is left to each House of Parliament to develop in the Standing Orders how to initiate Bills and other legislative processes. It is the 6th Respondent's contention that it would have

been different if the Constitution had imposed a limitation on this function or on the nomenclature of Bills to be determined by Parliament. The decision in the case of **Transparency International v Attorney General and 2 others**, HC Petition No. 388 of 2016 is cited in support of this submission.

659. The 6th Respondent submits that the Petitioners are simply calling upon the court to prescribe to the National Assembly what should be contained in the House Standing Orders. In his view, the remit of this court does not extend to the prescription of Standing Orders for the National Assembly. The case of **Nathanael Nganga Reuben v Speaker, Machakos County Assembly & another** [2016] eKLR is cited as holding that courts should exercise judicial restraint as regards Parliamentary and County Assembly proceedings which are closely and directly connected with the fulfilment by the Assembly or its members of their functions as a legislative and deliberative body.

660. The 6th Respondent buttresses the above contentions by submitting that the Supreme Court upheld the principle of allowing Parliament to regulate its internal matters in the case of **Speaker of the Senate & another v Attorney-General & 4 others** [2013] eKLR when it held that “[t]his Court will not question each and every procedural infraction that may occur in either of the Houses of Parliament” and that the “Court cannot supervise the workings of Parliament”. Also cited in support of the same proposition is the decision of this court in **Republic v National Assembly Committee of Privileges & 2 others Ex-Parte Ababu Namwamba** [2016] eKLR and that of the Court of Appeal in **Pevans East Africa Limited and Another v Chairman, Betting Control & Licencing Board and 7 others**, Civil Appeal No. 11 of 2018; [2018] eKLR.

661. The 6th Respondent submits that the use of omnibus Bills is not new to the National Assembly. He cites the Finance Bill which is passed every year and whose aim is to amend several laws that deal with revenue-raising measures or even repeal of entire taxation provisions as one of the Acts passed through the use of an omnibus Bill. It is his case that the amendments in a Finance Bill cannot be said to be minor amendments, and the same scenario applies to a Statute Law (Miscellaneous Amendment) Bill whose intention is to amend many statutes. His conclusion is that nothing bars Parliament from using a Statute Law (Miscellaneous Amendment) Bill as long as the principle of public participation is adhered to.

662. The 6th Respondent explains that among the reasons for the use of Statute Law (Miscellaneous Amendment) Bills by Parliament is the need to address backlogs in unlegislated areas and to save on parliamentary time. He contends that as admitted by the Petitioners, the Statute Law (Miscellaneous Amendment) Bill No. 12 of 2018 had objects and reasons, and a Memorandum of Objects and Reasons gives the intent and purpose of a Bill. In respect of the Statute law (Miscellaneous Amendment) Act (No. 18 of 2018 [Bill No. 12 of 2018] the objects and reasons were given as the making of “*various wide-ranging amendments on various statutes*” thus explaining the intent and purpose of the Bill.

663. The 6th Respondent’s final submission on the issue, however, is that the doctrine of separation of powers stops this court from entertaining the Consolidated Petitions. He supports his argument by citing Articles 117 and 124 of the Constitution and the Parliamentary Powers and Privilege Act of 2017. He further buttresses his contention by relying on the decision of the Court of Appeal in **John Harun Mwau v Dr. Andrew Mullei & Others**, Civil Appeal No. 157 of 2009, and that of the Supreme Court in the case of **Speaker of the Senate & another v Attorney-General & 4 others** [2013] eKLR. The

decision by the Privy Council in the New Zealand case of **Prebble v Television New Zealand Limited** [1995] 1 AC 32 is identified as illuminating the principle of separation of powers which requires that there be mutual respect between the courts and the legislature.

664. It is apparent from the submissions which we have set out above that the parties have expended considerable energy on the question of the place of omnibus (Statute Law Miscellaneous Amendment) Bills in enactment of legislation. The Petitioners are of the firm view that enactment of law through omnibus legislation should be reserved for minor, non-controversial and generally house-keeping amendments. The text they rely on is found in the **2016 Law Society Case** which has been cited numerous times before us. In its decision in that case, the court held as follows:

“234. It is therefore clear that both on policy and good governance, which is one of the values and principles of governance in Article 10 of the Constitution, which values and principles form the foundation of our State and Nation as decreed in Article 4(2) of the Constitution, omnibus amendments in the form of Statute Law Miscellaneous legislations ought to be confined only to minor non-controversial and generally house-keeping amendments.”

665. At this point we owe a duty to the parties and their advocates to place on record the fact that two members of this court (Mumbi Ngugi & W. Korir, JJ) were among the five members of the Bench that decided that case. It is also important to note that extensive discussions on the use of omnibus Bills in legislation were carried out in that case.

666. The Petitioners have also placed before this court the latest decision of the Court of Appeal on the issue. In a judgment delivered on 27th September 2019 in the **2019 Law Society Case**, the Court of Appeal (P. N. Waki, D. K. Musinga & P. O. Kiage, JJA) held that:

“It is imperative to dissect the issue of whether the amendments contained in the Statute Law Miscellaneous Amendments) Act, 2012, sought to introduce substantive amendments to the law. The issue turns on what is considered as substantive according to a reasonable man....

However, it is prudent to look at the ordinary usage of the Statute Law Miscellaneous Amendments) Bill. As was stated by the appellant and is clear from its long title, it professes and is meant to be “An Act of Parliament to make minor amendments to Statute Law”. From ordinary use of the word “minor” in this context, it means something that is of less importance, insignificant even. Indeed, the lexical meaning as obtained from the Concise Oxford English Dictionary, Twelfth Edition at page 911 is “having little importance, seriousness or significance”. The urging of the appellant is that the Statute Law (Miscellaneous Amendments) Bill is for correcting anomalies, inconsistencies, outdated terminologies or errors which are minor and non-controversial.

A quick look at Black’s Law Dictionary, Eighth Edition at page 1470, describes substantive law as;

“The part of the law that creates, defines, and regulates the rights and duties, and powers of parties.”

The Court must, therefore, satisfy itself that the amendments did not create, define, regulate or confer any powers to any parties, for if they did, they would not be said to be minor or inconsequential.”

667. Confronted with the said authorities the Respondents’ Counsel, and in particular Mr. Mwendwa for the 6th Respondent, changed tact and asked the Court to find that the decision of the Court of Appeal on the issue of the use of omnibus Bills was made *obiter dictum*. Mr. Mwendwa also reiterated his submission that directing Parliament not to use omnibus Bills in the enactment of substantive legislation amounts to chipping away the powers bestowed on Parliament by the people to legislate.

668. The decision of the Court of Appeal in the **2019 Law Society Case** may have answered the 6th Respondent’s concern about the alleged degradation of its legislative powers when it held that:

“In the case of judicial power, its derivation and vesting is provided for in Article 159 of the Constitution;

(1) Judicial authority is derived from the people and vests in, and shall be exercised by, the courts and tribunals established by or under this Constitution.

Similarly, Parliament’s legislative authority is neither innate nor self-authored. Rather, it is derived from and delegated to it by the people, is exercised on their behalf and must reflect their will in whom sovereignty resides.”

669. It is, however, our considered view that the 6th Respondent’s concerns need further interrogation. Before considering whether the Court can legitimately direct Parliament on the procedures it should employ to transact its business, we will first deal with the *obiter dictum* question. Counsel for the 6th Respondent, Mr. Mwendwa, sought to persuade us that the Court of Appeal decided the case based on the issue of public participation and not on the question of the use of an omnibus Bill to effect the amendments to the Law Society of Kenya Act which was the subject of litigation that gave rise to the appeal.

670. In **Ekuru Aukot v Independent Electoral & Boundaries Commission & 3 others** [2017] eKLR, Mativo, J dealt at length on the meaning and application of the principle of *obiter dictum* and concluded that:-

“43. The doctrine of precedent decrees that only the ratio decidendi [13] of a judgment, and not obiter dicta, have binding effect.[14] The fact that obiter dicta are not binding does not make it open to courts to free themselves from the shackles of what they consider to be unwelcome authority by artificially characterising as obiter what is otherwise binding precedent.[15] Only that which is truly obiter may not be followed. But, depending on the source, even obiter dicta may be of potent persuasive force and only departed from after due and careful consideration.”[16]

671. A perusal of the Court of Appeal judgment in the **2019 Law Society Case** discloses that the issue of the use of omnibus legislation was one of the grounds of appeal. The Court of Appeal identified the grounds of appeal in its judgment as follows:-

“The appellant, being dissatisfied with that judgment preferred an appeal to this Court. The memorandum of appeal contains three (3) grounds, complaining that the learned judge erred in law and in fact by;

a) Misdirecting himself by not finding that the amendments contained in the Statute Law (Miscellaneous Amendment) Act 2012 particularly those enumerated in paragraph 19(b) – 20 (b) – (d) of the Petition, are inconsistent with Articles 27,41 and 261 (4) of the Constitution.

b) Failing to appreciate that the amendments contained in the Statute Law (Miscellaneous Amendment) Act 2012 seek to introduce substantive amendments to the law.

c) Failing to appreciate the need for public participation as enshrined in Article 10 (2) as together with Article 118 of the Constitution before the enactment of the Statute Law (Miscellaneous Amendment) Act 2012.”
[Emphasis supplied]

672. The invitation to this Court to find that the decision of the Court of Appeal on the issue of the use of omnibus legislation was made in passing cannot be correct in such circumstances. The issue had been raised by the appellant. It was a matter for consideration by the Court of Appeal and was indeed decided upon. In the circumstances we find no substance in the claim by Counsel for the 6th Respondent that the question was dealt with in passing. We therefore reject the invitation to find that the decision of the Court of Appeal is not binding.

673. We come back to the question of the use of omnibus Bills in the legislative process. The High Court in the 2016 Law Society Case did extensive work on the issue and we need not cite the several authorities considered by the Court. It is, however, important to note that as observed in that case, there is no uniformity on how omnibus Bills are used in different jurisdictions:

“This brings to the fore the question of the circumstances under which statutory amendments ought to be effected by way of Statute Law Miscellaneous legislation. That such a procedure ought to avail only in cases of minor non-controversial amendments was appreciated by the 2nd Respondent when it indicated in the Memorandum of Objects and Reasons of the Bill....that....[t]he Statute Law (Miscellaneous Amendments) Bill, 2015 is in keeping with the practice of making minor amendments which do not merit the publication of a separate Bill and consolidating them into one Bill. .That this is the practice is clearly discernible from the practice adopted in most jurisdictions, though the practice is not consistent....While we appreciate that there is no internationally accepted position on the legality of omnibus bills, the reality is that they are used in many jurisdictions.”

674. There is indeed enough literature on the shortcomings associated with using omnibus Bills to effect substantive amendments to Acts of Parliament. Some of those shortcomings were captured in the 2016 Law Society Case in which the High Court cited a paper titled ***“Omnibus Bills in Theory and Practice”*** by Louis Massicotte published in the Canadian Parliamentary Review, Vol. 36 No. 1 2013, where the author states:-

“The real question, however, beyond the convenience of the government or of the opposition parties, may well be: is the public interest well served by omnibus bills” Take for example the clause-by-clause study in committee. When a bill deals with topics as varied as fisheries, unemployment insurance and environment, it is unlikely to be examined properly if the whole bill goes to the Standing Committee on Finance. The opposition parties complain legitimately that their critics on many topics covered by an omnibus bill have already been assigned to other committees. The public has every interest in a legislation being examined by the appropriate bodies.”

675. There is no doubt that the use of omnibus Bills to effect substantive amendments has its shortcomings. Such a process generally limits the right of the people to participate in the passing of laws. When Parliament proposes to make several amendments to assorted statutes relating to different activities, chances are that the proposals will not receive the kind of attention they should if they had been enacted through stand-alone Bills. The risk of excluding the public from participating in the legislative process is exacerbated if a short period for submitting views is provided. This risk was appreciated by **Louis Massicotte (supra)** as cited in the **2016 Law Society Case** in the passage that we have set out above. The use of omnibus Bills may have advantages for government for, as **Massicotte** observed:

“From the point of view of the government, omnibus bills have plenty of advantages....First, they save time and shorten legislative proceedings by avoiding the preparation of dozens of distinct bills necessitating as many second reading debates. Second, omnibus bills generate embarrassment within opposition parties by diluting highly controversial moves within a complex package, some parts of which are quite popular with the public or even with opposition parties themselves.

676. It is therefore apparent that the criticism of the omnibus Bill method is that it denies the public, including Parliamentarians, the opportunity to critically consider the proposed amendments and provide useful input. The limiting nature of the omnibus procedure has resulted in the courts discouraging the use of omnibus Bills to effect substantive amendments to legislation. Indeed in the **2016 Law Society Case** the court did not state that the legislature should not use omnibus Bills to carry out substantive amendments of statutes. What the court said is that *“omnibus amendments in the form of Statute Law Miscellaneous legislations ought to be confined only to minor non-controversial and generally house-keeping amendments.”* The key word here being *“ought”*.

677. In the **2019 Law Society Case**, the Court of Appeal seems to have taken issue with the fact that substantive amendments were effected through a Statute Law Miscellaneous Amendments Bill whose long title indicated that it was *“An Act of Parliament to make minor amendments to Statute Law”*. We are not persuaded that the Court of Appeal addressed the use of omnibus Bills in the legislative process and concluded that the procedure could not be used to make substantive amendments to Acts of Parliament.

678. From our analysis of the authorities above, we take the view that whenever the issue of the use of an omnibus Bill arises, the question to be posed is whether the procedure has, in the circumstances of the particular case, limited the right of the public to participate in the legislature’s business. In answering this question, the court will take into account the nature and extent of the amendments. An amendment that is controversial, involves the spending of

public funds, is likely to infringe the rights of persons or creates new offences will draw more attention from the court. The court will be interested to establish whether the use of the omnibus procedure limited the right of public participation.

679. However, if there is evidence placed before the court by the legislature to demonstrate that the principle of public participation was complied with in the adoption of the amendments, then the court should not be quick to hold such an amendment invalid simply because an omnibus Bill was used to make the amendments. It is not the place of the courts to dictate the procedures to be used by the two houses of Parliament in executing their legislative mandate. The business of the court is to confirm that the legislative bodies have complied with the Constitution and the law in delivering on their mandates.

680. This then brings us to the question whether the use of an omnibus Bill in the enactment of the impugned amendments negatively impacted on the right of the public to participate, thus necessitating a declaration of invalidity by this court. In this respect we have already found that there was evidence of sufficient time for public participation, and that the procedure employed by the 6th Respondent in the stakeholder engagement of the Omnibus Bill during the Committee Stage by various Committee, did facilitate public participation. In the circumstances, we find that the use of an omnibus Bill to enact the impugned legislation was not unconstitutional.

Whether the Bill was one concerning Counties and therefore required involvement of the Senate

681. The final issue relating to the procedural infirmities of the impugned amendments concern the question whether the amendments were on matters concerning counties and therefore required the involvement of the Senate. In answering this issue in the affirmative, the 1st Petitioner cites the case of **The Speaker of the Senate and Another and the Attorney General and Others** (2013) eKLR in which the Supreme Court held that if Parliament violates the procedural requirements of the supreme law of the land, it is for the courts of law to assert the authority and supremacy of the Constitution.

682. It is further the 1st Petitioner's case that for a law to be considered constitutional, it must be so both in form and content. The case of **Institute of Social Accountability & another v National Assembly & 4 others** [2015] eKLR is cited for the proposition that legislation must conform to the Constitution in terms of its content and the manner in which it was adopted. Failure to comply with the requirements in enacting legislation renders the legislation invalid.

683. The 1st Petitioner further cites the Supreme Court as stating in **The Speaker of the Senate and Another and the Attorney General and Others**, (*supra*) that the Senate ought to participate in the passing of a Bill as long as it can be shown that such a Bill has provisions affecting the functional areas of county governments. In support of the argument that the impugned amendments affected the operational areas of county governments, the testimony of Dr. Karanja Kibicho is cited as disclosing that NIIMS is intended to benefit county governments, and in particular on matters to do with food security, healthcare, housing and education.

684. Further, that the *Huduma Namba* will be needed to access services, including those offered by county governments. It is the 1st Petitioner's case that this is a clear indication that the impugned amendments related to matters concerning county governments, therefore necessitating the involvement of the Senate in the passage of the law. Reliance is again placed

on the decision in the **Institute of Social Accountability Case** for the proposition that failure to include the Senate in passage of a law touching on matters concerning county governments renders the law constitutionally infirm and invalid.

685. The 2nd Petitioner did not submit on the role of the Senate in the enactment of the Statute Law (Miscellaneous Amendments) Act 2018.

686. The 3rd Petitioner was, like the 1st Petitioner, of the view that the impugned amendments are unconstitutional as they were not referred to the Senate as required by Article 110 (2) (b) and (3), neither were they subjected to the mandatory provisions of Article 110(3) of the Constitution as the Speaker of the National Assembly and the Senate did not jointly resolve the question on whether the Statute law (Miscellaneous Amendment) Bill 2018 was a Bill concerning counties. According to the 3rd Petitioner, the conduct of the National Assembly undermined the legal structure and framework of the legislature and the established procedure for enacting legislation. The decision of the Supreme Court in **The Speaker of the Senate and Another and the Attorney General and Others**, (supra) is cited as having conclusively dealt with the question of the roles of the National Assembly and the Senate with regard to the organization, introduction and consideration, and enactment of Bills. It is the 3rd Petitioner's case that the Supreme Court held that the Senate, though entrusted with a less expansive legislative role than the National Assembly, stands as the Constitution's safeguard for the principle of devolved government.

687. It is further the 3rd Petitioner's contention that Article 93 establishes Parliament comprising the National Assembly and the Senate with each House enjoined to perform its respective functions in accordance with the Constitution. It contends that where the Constitution prescribes a procedure that ought to be followed in enacting a law, that procedure must be followed. The decision in the **Doctors For Life Case** is relied upon in support of the principle that legislation must conform to the Constitution both in terms of its content and the manner in which it is adopted, and failure to comply with the requirements in enacting legislation renders the legislation invalid.

688. The 5th Interested Party supports the position taken by the Petitioners that the Statute law (Miscellaneous Amendment) Bill 2018 was a Bill concerning counties and the involvement of the Senate in the legislative process was required. It relies on Article 110(3) of the Constitution and cites the decision in **The Speaker of the Senate and Another and the Attorney General and Others**, (supra) as holding that the Speaker of the Senate should be consulted in classification of Bills. It is its submission that in this case, there is no evidence that the Speaker of the Senate was consulted and determined that the Bill was not one concerning county governments.

689. The 5th Interested Party also relies on the case of **Re the Matter of the Interim Independent Electoral Commission, Supreme Court Const. Appl. No. 2 of 2011** in which the Supreme Court advised that the expression '*any matters touching on county government*' should be so interpreted as to incorporate any national level process bearing a significant impact on the conduct of county governments. It is its position that a Bill concerning counties is therefore one that fits the definition of Article 110 of the Constitution and also has an impact on the conduct of county governments.

690. To justify its assertion that the impugned amendments concerned counties, the 5th Interested Party submits that the main stated benefit of NIIMS is to ease delivery of services to the people. It observes that similarly, some of the purposes of devolution and the creation

of county governments according to Article 174 of the Constitution are the promotion of social and economic development and the provision of proximate, easily accessible services throughout Kenya; and facilitation of the decentralisation of State organs, their functions and services, from the capital of Kenya. It therefore asserts that if NIIMS is meant to be a tool to provide easier access to services and the purpose of devolution is to do the same thing, then the Senate ought to have been consulted in the enactment of a legislation that encroaches on their function.

691. It is therefore the 5th Interested Party's firm position that the failure by the National Assembly to involve the Senate in the legislative process in a Bill that concerned the county government makes the resulting legislation null and void. The decision in the **Institute of Social Accountability Case** is cited in support of the assertion that failure to involve the Senate in the enactment of an Act concerning county governments renders such an Act unconstitutional.

692. The 6th Interested Party did not make any submission on the issue of the non-involvement of the Senate in the legislation of the impugned amendments.

693. The Respondents vehemently oppose the position taken by the Petitioners and the Interested Parties who support them on the role of the Senate with respect to the impugned amendments. The 1st Respondent submits that Article 109(1) of the Constitution mandates Parliament to legislate through Bills that are eventually assented to by the President. He asserts that Article 109(3) of the Constitution provides that a Bill not concerning county governments is considered only in the National Assembly and Article 109(1) defines '*a bill concerning county governments*' to include Bills containing provisions affecting the functions and powers of county governments as set out in the Fourth Schedule, Bills relating to election of members of county assembly or county executive and Bills affecting finances of county governments.

694. Applying the cited law to the facts of this case, the 1st Respondent submits that national registration and data and statistics are national government functions as they are not enumerated in Part 2 of the Fourth Schedule which sets out the functions of county governments.

695. The 2nd and 3rd Respondents agree with the position taken by the 1st Respondent, contending that the Bill did not warrant consideration by the Senate. In their view, the fact that a proposed amendment may tacitly confer incidental benefits to county governments does not make such a Bill a Bill "*concerning county governments*." They rely on the Court of Appeal definition of a "*bill concerning county governments*" in the case of **National Assembly of Kenya & Another v Institute for Social Accountability & 6 Others** [2017] eKLR. In their view, the registration of persons is a function that falls within the category of national statistics and data on population which is a function reserved for the national government pursuant to section 11 of the Fourth Schedule of the Constitution.

696. We have considered the respective submissions of the parties on the question whether the Senate had a role in the enactment of the impugned amendments. We note that the parties are agreed that the impugned amendments were originated and passed by the National Assembly without reference to the Senate. The only question therefore is whether the impugned amendments concerned county governments and could only pass with the approval of the Senate.

697. The Supreme Court extensively dealt with this issue in The **Speaker of the Senate and Another and the Attorney General and Others**, (supra) which has been extensively cited before us by the parties. Although the question of whether the procedure of determining if a Bill concerns county governments is not one of the issues before this court, for purposes of determining the issue before us, we find it necessary to highlight what the Supreme Court stated, which is as follows:

“[141] It is quite clear, though some of the counsel appearing before us appeared to overlook this, that the business of considering and passing of any Bill is not to be embarked upon and concluded before the two Chambers, acting through their Speakers, address and find an answer for a certain particular question: What is the nature of the Bill in question” The two Speakers, in answering that question, must settle three sub-questions – before a Bill that has been published, goes through the motions of debate, passage, and final assent by the President. The sub-questions are:

a. is this a Bill concerning county government” And if it is, is it a special or an ordinary bill”

b. is this a bill not concerning county government”

c. is this a money Bill”

[142] How do the two Speakers proceed, in answering those questions or sub-questions” They must consider the content of the Bill. They must reflect upon the objectives of the Bill. This, by the Constitution, is not a unilateral exercise. And on this principle, it is obvious that the Speaker of the National Assembly by abandoning all engagement or consultation with the Speaker of the Senate, and proceeding as he did in the matter before this Court, had acted contrary to the Constitution and its fundamental principles regarding the harmonious motion of State institutions.

[143] Neither Speaker may, to the exclusion of the other, “determine the nature of a Bill”: for that would inevitably result in usurpations of jurisdiction, to the prejudice of the constitutional principle of the harmonious interplay of State institutions.

[144] It is evident that the Senate, though entrusted with a less expansive legislative role than the National Assembly, stands as the Constitution’s safeguard for the principle of devolved government. This purpose would be negated if the Senate were not to participate in the enactment of legislation pertaining to the devolved units, the counties [Article 96(1), (2) and (3)].

[145] It is clear to us, from a broad purposive view of the Constitution, that the intent of the drafters, as regards the exercise of legislative powers, was that any disagreement as to the nature of a Bill should be harmoniously settled through mediation. An obligation is thus placed on the two Speakers, where they cannot agree between themselves, to engage the mediation mechanism. They would each be required each to appoint an equal number of members, who would deliberate upon the question, and file their report within a specified period of time. It is also possible for the two Chambers to establish a standing mediation committee, to deliberate upon and to resolve

any disputes regarding the path of legislation to be adopted for different subject-matter.”

698. The Supreme Court explained the role of the Senate in the passage of Bills by stating that:-

“[102] The Court’s observation in Re the Matter of the Interim Independent Electoral Commission is borne out in an official publication, Final Report of the Task Force on Devolved Government Vol. 1: A Report on the Implementation of Devolved Government in Kenya [page. 18]:

“The extent of the legislative role of the Senate can only be fully appreciated if the meaning of the phrase ‘concerning counties’ is examined. Article 110 of the Constitution defines bills concerning counties as being bills which contain provisions that affect the functions and powers of the county governments as set out in the Fourth Schedule; bills which relate to the election of members of the county assembly or county executive; and bills referred to in Chapter Twelve as affecting finances of the county governments. This is a very broad definition which creates room for the Senate to participate in the passing of bills in the exclusive functional areas of the national government, for as long as it can be shown that such bills have provisions affecting the functional areas of the county governments. For instance, it may be argued that although security and policing are national functions, how security and policing services are provided affects how county governments discharge their agricultural functions. As such, a bill on security and policing would be a bill concerning counties....With a good Speaker, the Senate should be able to find something that affects the functions of the counties in almost every bill that comes to Parliament, making it a bill that must be considered and passed by both Houses.”

699. On its part, this Court (Lenaola, J (as he then was) Ngugi & Majanja JJ) in the Institute of Social Accountability Case cited above stated that:-

“66. Accordingly it is clear that if the Speaker of the Senate signifies concurrence with a Bill that it falls within one category or another, it may well be said that would be the end of the matter. However, the issue whether the matter is one for county government is of constitutional importance and the decision of the respective speakers, while respected, cannot be conclusive and binding on the court whose jurisdiction it is to interpret the Constitution and as the final authority on what the Constitution means. Participation of the Senate in the legislative process is not just a matter of procedure, it is significant to the role of the Senate in our constitutional scheme as the Senate’s legislative role is limited to matters concerning county governments. Through its participation in the legislative process, the Senate is seized of the opportunity to discharge its primary mandate which is, to protect the interests of the counties and county governments as mandated under Article 96(1) of the Constitution. It is a means of ensuring that the county voice is heard and considered at the national forum and the interests of counties and their governments secured. This way, the sovereign power of the people is duly exercised through their democratically elected representatives.

Therefore, when the speakers of both chambers classify bills under Article 110, they are essentially resolving on the question as to whether and to what extent provisions of a particular Bill affect the interests of county governments, and consequently whether county input ought to be invited....

69. In our view and we so hold, the fact that the legislation was passed without involving the Senate and by concurrence of the Speakers of both House of Parliament, is neither conclusive nor decisive as to whether the legislation affects county government. In other words, while concurrence of the Speakers is significant in terms of satisfaction of the requirements of Article 110(3) of the Constitution, it does not by itself oust the power of this Court vested under Article 165(3)(d) where a question is raised regarding the true nature of legislation in respect to Article 110(1). The court must interrogate the legislation as a whole and determine whether in fact the legislation meets the constitutional test of a matter, “concerning county government.” We shall revert to this issue when we review the substance of the CDF Act and the subsequent amendment to determine whether in fact the legislation is a matter concerning county government.”

700. The Court proceeded to determine that:

“138. We have analysed the CDF Act and concluded that the CDF and the manner it is administered and projects implemented impacts functions allocated to the county under the Fourth Schedule to the Constitution. In terms of Article 96(2) and 110 of the Constitution, the CDF (Amendment) Bill as legislation affecting the functions and powers of the county governments qualifies as, ‘a Bill concerning county government’ within the meaning of Article 110(1) and ought to have passed by the Senate. The purpose of the CDF (Amendment) Act was to amend a law that as we have found violates the division of functions between the national and county governments. Thus, an amendment to the Act would have necessitated the input of the Senate. The purpose of involving the Senate is to ensure that counties, as far as possible, get to effectively participate in the legislative business at the national level in matters substantially affecting interests of county governments. This calls for the court to look beyond the substance or purpose of the statute expressed in the text. The court must unbundle the specific provisions of the proposed legislation to see if and to what extent they satisfy the criteria set out under Article 110(1) of the Constitution. An amendment to the Act affecting the manner in which money is allocated to the CDF is the core part of the Act. As the availability of money affects the financing and implementation of projects that fall within the competence of the county government, the provision cannot be severed without undermining the entire Act. The CDF (Amendment) Bill is not an insubstantial amendment. We therefore find and declare that the CDF (Amendment) Bill unconstitutional for want of involvement by the Senate and we so declare.”

701. As we understand it, the term “concerning counties” has a wide meaning. According to the Supreme Court, the phrase:

“...creates room for the Senate to participate in the passing of bills in the exclusive functional areas of the national government, for as long as it can be shown that such bills have provisions affecting the functional areas of the county governments.”

702. We, however, do not think that the jurisdiction of the Senate extends to each and every legislation passed by the National Assembly. To so hold would render Article 110 of the Constitution redundant. It is difficult to think of any legislation that does not touch on counties. The Fourth Schedule of the Constitution does indeed give a wide array of functions to the counties. Those functions, in our view, do not include a national population register. It is therefore our finding and holding that the impugned amendments did not require the involvement of the Senate in their enactment. That is not to say that the bill should not have been subjected to the procedure identified by the Supreme Court in **The Speaker of the Senate and Another and the Attorney General and Others**, (supra).

703. In closing on this issue, we observe that while the Petitioners have argued that the Bill was not subjected to the process enunciated by the Supreme Court in **The Speaker of the Senate and Another and the Attorney General and Others**, (supra), the issue was not in their pleadings. As expected, therefore, the Respondents did not reply to it. It would therefore be unfair to make a determination on it in light of the principle of the right to a hearing.

704. It is our finding therefore and we so hold that, in light of the above analysis, the impugned amendments did not concern counties. As such, we find no merit in the Petitioners' case that the impugned amendments failed the constitutional test for non-involvement of the Senate in the process of their enactment.

Whether there is Violation and/or Threatened Violation of the Right to Privacy.

705. All the Petitioners urged on the risks and threats of the impugned amendments and of NIIMS to the right to privacy, and of the insufficiency of the legal protection of the personal information collected through NIIMS. The Respondents countered these averments by *inter alia* explaining that the design of NIIMS will ensure adequate security of data collected and that there are existing laws for data protection. The arguments made by the parties in this regard have been collapsed to four sub issues:

(a) Whether the personal information collected pursuant to the impugned amendments to the Registration of Persons Act is excessive, intrusive, and disproportionate to the stated objectives of NIIMS.

(b) Whether there are sufficient legal safeguards and data protection frameworks for the personal information that is collected in NIIMS

(c) Whether the impugned amendments to the Registration of Persons Act are an unreasonable and unjustifiable limitation to the right to privacy;

(d) Whether NIIMS complies with the peremptory constitutional principles of transparency, accountability, and verifiability and whether it is secure for its intended purpose.

Whether the personal information collected is excessive, intrusive, and disproportionate.

706. There were two limbs of arguments raised as regards this issue. The first limb was that the provisions for collection of biometric data by the impugned amendments was intrusive

and unnecessary. The 1st Petitioner in this respect urges that DNA and other forms of biometric data are listed by the impugned amendments, without justification or limitation, which clearly contravenes the principle of data minimization. That this is so particularly given that NIIMS is being populated without DNA, and the government has publicly stated multiple times that it lacks the capacity to store this data and to process it.

707. Further, that the Digital Data Capture Form used to gather biographical information is extremely detailed and extensive. The 1st Petitioner submits that in the context of general collection of biometric data outside of the criminal law context, it is likely to result in violations of fundamental rights unless there are very strict and rigorous safeguards. This is for the reason that once there is a breach of the database, the information taken is unlikely to be recovered in full. Therefore, there being no restrictions on retention of data in law, or in the design and public information concerning the administration of NIIMS, the NIIMS database is intrusive.

708. Lastly, the 1st Petitioner argues that the Respondents have failed to indicate why collection of biometric information is necessary at all, beyond distinguishing Kenya from Estonia on the basis of population “heterogeneity” which purportedly justifies “a more robust identity system”, without explaining why biometrics would be better-suited to the Kenyan context, and why specifically 10 fingerprints are needed.

709. The 2nd Petitioner on its part submits that the right to privacy is an inherent right of every person and is not granted by the State, but entrenched as a fundamental right that cannot be lightly diluted, infringed and/or interfered with by the State without proper justification. The 2nd Petitioner relies on the decision of Chelameswar, J. in **KS Puttaswamy vs Union of India Writ Petition (Civil) No 494 of 2012**, as was cited by the Jamaican Supreme Court in **Julian J Robinson vs The Attorney General of Jamaica, Claim No. 2018 HCV01788**, which underscored the fundamental status of rights protected under the bill of rights and specifically the right to privacy as one of the core freedoms which is to be defended.

710. The 2nd Petitioner also relies on the case of **Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others vs Cabinet Secretary Ministry of Health & 4 Others**, [2016] eKLR where Lenaola J (as he then was) defined privacy as a high level of protection given to the individual’s intimate personal sphere of life.

711. The 2nd Petitioner further submits that the full import of biometric data is to require all persons to surrender their unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid (DNA) in digital form, Global Positioning Systems coordinates, Land Reference Number, and their Plot Number or House Number, if any. In its view, biometric personal information to be obtained under the impugned amendments is not only profoundly intrusive compared to the hitherto physical/manual information, it is also inherently susceptible to the risk of invasion by unintended third parties and may be used for innumerable unintended purposes.

712. Further, that the Supreme Court of India (Dr. Chandrachud J) in the case of **KS Puttaswamy vs Union of India** (*supra*) cited by the Supreme Court of Jamaica in **Julian J Robinson vs The Attorney General of Jamaica** (*supra*) aptly captures the character of biometric data relative to privacy in that, when adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance.

713. The 2nd Petitioner also urges that privacy ensures autonomy and self-determination in the face of increasing State power, and that data collection and analysis can be a demoralizing process and can create a false image of an individual. Thus, broad government access to an individual's information can significantly upset the delicate balance of power in a democracy between citizen and State. The 2nd Petitioner's contends that no evidence has been provided by the Respondents to support the assertion that biometric data is the most robust authentication and identification method available, or that there were no alternative/less intrusive means of achieving the stated purpose of NIIMS.

714. The 3rd Petitioner reiterates that the impugned amendments will enable the Respondents to collect personal data which qualifies as sensitive personal information which would require consent, clear objectives for collection, measures to protect the information from any breaches and remedies for breach. However, that the amendments do not provide for any of the above thereby exposing individuals to violation of their privacy guaranteed under Article 31 of the Constitution.

715. The 5th Interested Party on its part submits that all the information required under NIIMS was unnecessary as this is information that exists in other State databases that is, the information collected under NIIMS is identical to the information kept by the Principal Registrar under Section 5 of the Act. Be that as it may, that all the information sought in the Huduma Namba Data Capture Form amounts to information relating to one's family and one's private affairs.

716. The 5th Interested Party further submits that Section 3 of the Registration of Persons Act was amended to include the definition of "biometric" as unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form. To that end, it cites the case of **Julian J Robinson vs The Attorney General of Jamaica [2019] JMFC Full 04** (hereinafter the **Julian Robinson Case**), where the Supreme Court of Jamaica noted that biometric data, by its very nature, is intrinsically linked to characteristics that make us 'humans' and its broad scope brings together a variety of personal elements and the collection, analysis and storage of such innate data is dehumanising as it reduces the individual to but a number. Further, that when an individual is forced to surrender a biometric identifier as part of State action, they are giving up information about themselves and they disclose truly unique information about their identity among others.

717. The 5th Interested Party also cites the case of **Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others [2016] eKLR** where while considering the problematic aspects of government databases, Lenaola J (as he then was) and Muriithi J held that even where the goal being pursued by the State is legitimate, the manner in which data is collected can be an infringement on the right to privacy.

718. It is the 5th Interested Party's view that data was collected without informed consent from the data subjects and this being a State-backed exercise, it cannot be said that those who gave their information understood what they were doing nor can it be said that they gave informed consent to the utilisation of their information. Further, that the Data Capture Form, and indeed a lot of government propaganda which this court must take judicial notice of, came with a warning "*Huduma Namba Registration is mandatory as per Section 9A of the Registration of Persons Act (Cap 107). It will enable the Government to provide you with*

services”, which amounts to deliberately misleading the public as no reading of section 9A would produce the interpretation stated in the Data Capture Form nor does it make it compulsory for people to register for the said *Huduma Namba* or even tie the registration of this number to the provision of services. Accordingly, if indeed more than 31 million people registered under NIIMS, they did so under duress and fear of the unknown drove them to register, not their autonomy.

719. Closely related to the first limb of the issue at hand is the second limb that that the data collected pursuant to the impugned amendments is not supported by the stated purposes of NIIMS and is purpose free. The 1st Petitioner submits in this regard that the principle of purpose limitation is to form a consensus view of the purpose of data collection, which in their view does not exist in this case. It further submits that data collection for the purposes of crime fighting, surveillance or countering terrorism is counterproductive to data collection for the purpose of service delivery. Nevertheless, it was its submission that the Respondents variously claim all three and more. Further, because the Data Capture Form was so extensive and the purposes of the NIIMS system so opaque, there was no reliable way to know the specific purpose of each piece of data collected for a given individual, and to track whether the data are only used for that purpose.

720. The 1st Petitioner contends that the impugned amendments do not state a single, specific purpose of NIIMS, and that the Respondents’ replying affidavits and expert evidence take contradictory positions with regard to the purpose and effect of the NIIMS system, and its relationship to other existing identification infrastructure. For example, that the 5th Respondent’s response to the petition of the Kenya National Commission on Human Rights states that NIIMS will eliminate vetting for national identity cards, but the “*Digital Data Capture*” form does not collect sufficient information to determine nationality, nor were the registration officials performing enrolments competent to make such determinations, when in fact Kenyan law does not currently provide for any reliable legal or administrative means of confirming citizenship by birth. Meanwhile, the 2nd Respondent states that “NIIMS will not replace the previous registration systems in the short term.”

721. That the Respondents, furthermore, repeatedly state that DNA was not collected, while also affirming that DNA data is essential for posthumous identification and the prevention of child trafficking and terrorism, two important capabilities of the NIIMS system. Moreover, unlike other foundational digital identity systems, NIIMS boasts forensics and crime fighting among its purposes, with the most-cited purpose, being improved service delivery, relegated lower on the list. Accordingly, the amendment itself does not specify or restrict the potential purposes of the NIIMS system in any way, nor does it provide an exhaustive list of the potential functions of the NIIMS system itself.

722. The 2nd Petitioner submits that the averments by the Respondents on the stated benefits of NIIMS erroneously presuppose that the stated challenges stem from the lack of a unique identification number, and that unless NIIMS is operationalized in its current form and with the aid of criminal sanctions, then the challenges will persist. However, they submitted that no empirical or other evidence has been adduced in support of this assertion or that less invasive alternatives were considered and/or were unavailable to achieve the same objective, and no such alternatives were even discussed. Reference was made to the decision by the Supreme Court of Jamaica in the **Julian Robinson Case** where it addressed a similar situation.

723. It was the 2nd Petitioner's submission that the African Union Convention on Cyber Security and Personal Data Convention adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014 (hereafter "The Malabo Convention") stresses the protection of personal data, and urges a balance between the use of information and communication technologies and the protection of the privacy of citizens. It is pursuant to the said convention that the Data Protection Bill was sponsored and in line with the Malabo Convention, the Data Protection Bill 2018 proposes among other safeguards the creation of an independent Data Protection Authority, specifically, the Kenya National Commission on Human Rights, which is a Constitutional Commission established under Section 3 of the Kenya National Commission on Human Rights Act No. 14 of 2011.

724. On the issue that collection of DNA is justified and necessary for crime prevention including child trafficking, the 2nd Petitioner submits that no empirical evidence has been adduced by the Respondents to justify the claim that NIIMS will prevent child trafficking or that countries that have managed to curb trafficking have done so by using a unique identifier or biometric personal data. In their view, taking measures to address the foregoing challenges would be less intrusive alternatives of achieving the stated objectives of NIIMS. In any event, the 2nd Petitioner submits, existing criminal laws such as sanctions prescribed by the Kenya Information and Communications Act, the Computer Misuse and Cybercrimes Act of 2018 and the Access to Information Act are not sufficient deterrents for the protection of personal data. It was its argument that once personal data is breached and misused, the devastating effects such loss would have on data subjects cannot be remedied by any amount of criminal punishment against the offender and the court in the **Julian Robinson Case** eruditely captured this problem by stating that there must be robust systems that minimise data theft and the punishment for data misuse and abuse must be such that there is a strong deterrent element in the data protection regime.

725. On the argument that NIIMS was established for purposes of compliance with Kenya's time bound international obligations pursuant to section 17(3)(c) of the Access to Information Act, the 2nd Petitioner submits that there is no correlation to support the argument that mandatorily collecting biometric information of the nature prescribed by the impugned amendments is at all necessary for purposes of computerizing records and information management systems or to facilitate more efficient access to information. It was further its submission that collection of biometric data is a new phenomenon under the Registration of Persons Act and the risks attendant to storing the biometric data in a central database is subjecting it to manipulation with the possibility of generation of new data which risk was highlighted in the **Julian Robinson Case**.

726. The 3rd Petitioner's relies on the case of **Institute of Social Accountability & another v National Assembly & 4 others** (*supra*) which cited with approval the Canadian Supreme Court in the **R vs Big M Drug Mart Ltd** (*supra*) which stated that both purpose and effect are relevant in determining constitutionality; either an unconstitutional purpose or an unconstitutional effect can invalidate legislation. That there is therefore a real threat that NIIMS is susceptible to breach that would occasion irreparable harm and damage to the people, and indeed the country at large.

727. The 5th Interested Party submits in support of the Petitioners that to determine the purpose of a legislation, a court must be guided by the object and purpose of the impugned statute, which object and purpose can be discerned from the legislation itself as was stated by the court in **Geoffrey Andare v Attorney General & 2 Others**, [2016] eKLR. However, if Petition 56, 58 & 59 of 2019 (Consolidated) | Page 139 of 205.

the purpose is not clear from the Act, then this Court has the discretion to interrogate the Hansard to determine the legislative intent. Any other source of information is speculative and conjecture at best. Further, that Section 7 of the Sixth Schedule to the Constitution offers guidance that laws such as this one must be construed with the alterations, adaptations, qualifications and exceptions necessary to bring it into conformity with this Constitution.

728. The 5th Interested Party further submits that even if the purposes explained in the Respondents' pleadings were contained in the legislation, the same would not constitute a constitutional purpose. In the 5th Interested Party's view therefore, NIIMS is a superfluous system serving no specific purpose, and its potential harms far outweigh any peripheral advantages. Consequently, the court was urged to find that if any activity is to be done under NIIMS, a proper legislative direction must be given detailing its purpose, safeguards to be used and in line with both Article 31 and Article 24 of the Constitution.

729. The Respondents replied to the arguments made on the nature and need of the data in NIIMS in their submissions. With particular respect to unique identifiers or attributes including fingerprints, location information, land reference number, postal address, and GPS coordinates, the 1st Respondent submits that such information is a standard requirement all over the world, and are not in any way disproportionate to the legitimate aims of the State. Further to that, the requirement for GPS location is to comply with section 5(g) of Registration of Persons Act, and merely have a geographical expression of the location of a physical place for information purposes with a primary objective of facilitation of government services. To buttress the instances when the right to privacy can be limited, the 1st Respondent urges the Court to find persuasion in the reasoning of the High Court in **Coalition for Reform and Democracy (Cord) & 2 Others V Republic of Kenya & 10; Others [2015] eKLR** where it was held that the right to privacy can never be absolute, and that a balancing test has to be applied to determine whether the intrusion into an individual's privacy is proportionate to the public interest to be served by the intrusion.

730. It was his submission that sensitive information such as tribe, race, HIV status, among others specifically stood excluded, and that following this Court's orders of 1st April, 2019, the only biometric information that was actually collected during the pilot phase and the mass registration exercise was only limited to the fingerprints, which is considered to be the core biometric information. That it is frequently utilized globally to ascertain the identity of a person. In that regard, they submitted that the information gathered was and is actually non-invasive and non-intrusive identity information.

731. The 1st Respondent cites the decision by the Indian Supreme Court decision in **Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others Writ Petition (Civil) No. 494 of 2012**, where it was held that demographic information, both mandatory and optional, and photographs does not raise a reasonable expectation of privacy unless under special circumstances such as juveniles in conflict of law or a rape victim's identity. Further, that it was held that there is no reasonable expectation of privacy with respect to fingerprint and iris scan as they are not dealing with the intimate or private sphere of the individual but are used solely for authentication.

732. In addressing children's privacy concerns, it was the 1st Respondent's submission that implementation of NIIMS would be in the best interests of children, for the simple reason that it will enable the State to fulfil its constitutional obligations of protecting and promoting, *inter alia*: children's' right to free and compulsory basic education; basic nutrition, shelter and

healthcare; to be protected from abuse, neglect, harmful cultural practices, all forms of violence, inhuman treatment and punishment; and hazardous or exploitative labour as under Article 51(1) of the Constitution.

733. In regard to the claim that collection of DNA identity data exercise is too intrusive and would violate the privacy of data subjects, the 1st Respondent contends that the practice is permissible in Kenya, as held in **L.N.W. v. Attorney General & 3 Others** [2016] eKLR where it was held that there is need for provision for DNA testing to be undertaken to establish paternity where it is denied.

734. The 4th and 7th Respondents on their part submit that the personal information collected through NIIMS is of a similar nature as that currently being held by various government agencies. Further, that the purpose is to integrate and consolidate the information in order to create, manage and operate a digitized national population register as a single source of personal information on all Kenyan citizens and residents. It was also submitted that the information will assist the government to meet its obligation of providing key services to its citizens including security, healthcare, and education among others

735. According to the 4th and 7th Respondents, the Petitioners' grievance is with the collection of DNA and GPS information. With respect to DNA, they submitted that it is a unique identifier that is not part of the personal information collected by the data capture tools for purposes of registration under NIIMS. Further to that, they submitted that GPS coordinates and DNA information were not collected by the data capture tools in place during the mass registration exercise pursuant to this Court's ruling of 1st April, 2019,

736. The said Respondents however still submitted on the importance of collecting DNA and GPS, and contended that such information would be critical in enabling many technologies, and that the collection of personal information of citizens is central to the proper functioning of the State. To that end, reference was made to the United States Supreme Court case of **Margaret O'Hartigan vs Department of Personnell ET AL** 118 Wn. 2d 111, P2d 44 (No. 56063-3 En Banc) where it pointed out that disclosure of intimate information to governmental agencies is permissible if it is carefully tailored to meet a valid governmental interest, and provided the disclosure is no greater than is reasonably necessary. The 4th and 7th Respondents therefore submit that the government interest in collecting information through NIIMS is in keeping State's duty of care to its citizens, and that vital and reliable data is central to the discharge of this duty.

737. It was also their submission that the Petitioners failed to adduce any evidence to demonstrate the manner in which the collection of personal information is an "unnecessary requirement" as set out in Article 31 (c) of the Constitution, especially in light of the fact that the information is already held by the State, albeit in different institutions. They further claimed that the Petitioners do not challenge any other statutory provisions which allow the government to collect personal information on account of an alleged infringement to the right to privacy.

738. The 5th Respondent submits that the amendment complained of does not limit or violate the right to privacy as alleged, and only captures necessary biometric information in line with globally acceptable requirements in securing the State against terrorism, money laundering and to aid national planning. Further, that the right to privacy is only violated when unauthorized persons gain access to the data under protection. In this instance, that government officers legitimately gain access for a lawful purpose.

739. The 8th and 9th Interested Parties' submissions were on the role of digital identification in sustainable development. The said Interested Parties note that following the adoption and ratification of the Sustainable Development Goals in 2015, various multilateral and international organizations, including the World Bank, UNDP and UNICEF, to which Kenya is a member, have all stressed the critical role played by digital identity databases in realizing the said Goals which are in many ways similar and/or identical to the national values and principles of governance under Article 10 of the Constitution of Kenya.

740. The 8th and 9th Interested Parties make reference to various publications that have found that lack of personal official identification prevents people from fully exercising their rights and isolates them socially, economically and politically. Further, that beyond quantifiable economic benefits, digital ID can offer non-economic value to individuals through social and political inclusion, rights protection and transparency. Therefore, that the right digital identification technology designed with the right principles and enforced with the right policies, can be used in the provision of e-government services and benefits, expanding access and saving time for citizens while reducing costs for governments and improving social welfare.

741. In addressing these two related limbs, this Court is mindful of the provisions of Article 31 of the Constitution on the right to privacy, which provide as follows:

“Every person has the right to privacy, which includes the right not to have—

(a) their person, home or property searched;

(b) their possessions seized;

(c) information relating to their family or private affairs unnecessarily required or revealed; or

(d) the privacy of their communications infringed.”

742. The Article therefore guarantees a general right to privacy, and in addition also guards against specific infringements of privacy, including unnecessary revelation of information relating to family or private affairs, which is the bone of contention in the consolidated petitions herein. The South African Constitutional Court discussed the elements and scope of the general right to privacy in Bernstein vs Bester NO (1996) 2 SA 751 (CC), wherein Ackermann J. held as follows in the majority judgment in paragraph 67:

“(67).....The truism that no right is to be considered absolute, implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.”

743. The learned Judge went to on to give examples of what is commonly considered an intrusion of the right to privacy as follows in paragraphs 68 to 69:

“(68)....Privacy is an individual condition of life characterised by seclusion from the public and publicity. This implies an absence of acquaintance with the individual or his personal affairs in this state. In Financial Mail (Pty) Ltd v Sage Holdings Ltd ([1993] ZASCA 3; 1993 2 SA 451) it was held that breach of privacy could occur either by way of an unlawful intrusion upon the personal privacy of another, or by way of unlawful disclosure of private facts about a person. The unlawfulness of a (factual) infringement of privacy is adjudged in the light of contemporary boni mores and the general sense of justice of the community as perceived by the Court.

(69) Examples of wrongful intrusion and disclosure which have been acknowledged at common law are entry into a private residence, the reading of private documents, listening in to private conversations, the shadowing of a person, the disclosure of private facts which have been acquired by a wrongful act of intrusion, and the disclosure of private facts contrary to the existence of a confidential relationship. These examples are all clearly related to either the private sphere, or relations of legal privilege and confidentiality. There is no indication that it may be extended to include the carrying on of business activities.”

744. The learned Judge concluded that the scope of a person’s privacy extends only to those aspects in regard to which a legitimate expectation of privacy can be harbored. In this respect, it was held that a person’s subjective expectation of privacy is subject to the test that the society recognises that expectation to be objectively reasonable.

745. This position was adopted by the Kenyan Courts in **Roshanara Ebrahim v Ashleys Kenya Limited & 3 Others**, [2016] eKLR, **Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others**, [2016] eKLR, and in **Tom Ojienda t/a Tom Ojienda & Associates Advocates v Ethics and Anti-Corruption Commission & 5 others** [2016] eKLR. It is notable that section 13 of the South African Interim Constitution which was the basis of the decision in **Bernstein vs Bester** was similar to Article 31 save for the protection of informational privacy, and stated as follows:

“Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications.”

746. In **Tom Ojienda t/a Tom Ojienda & Associates Advocates vs Ethics and Anti-Corruption Commission & 5 others** (*supra*) it was held as follows in this regard:

“77. I also note that a legitimate expectation of privacy has two components; the protection of the individual and the reasonable expectation of privacy. The reasonable expectation of privacy test itself has two compartments. Firstly, there must be at least a subjective expectation of privacy and secondly, the expectation must be recognized as reasonable by the society.....

78. Ackermann J’s reasoning can therefore be summarized as follows; (a) privacy is a subjective expectation of privacy that is reasonable, (b) it is

reasonable to expect privacy in the inner sanctum, in the truly personal realm, (c) a protected inner sanctum helps achieve a valuable good—one's own autonomous identity. It emerges to my mind that, and from the decision in Bernstein vs Bester NO (supra), that privacy is not a value in itself but is valued for instrumental reasons, for the contribution it makes to the project of 'autonomous identity'. This protection in return seeks to protect the human dignity of an individual."

747. The right to privacy has also been expressly acknowledged in international and regional covenants on fundamental rights and freedoms. It is provided for under Article 12 of the Universal Declaration on Human Rights, Article 17 of the International Convention on Civil and Political Rights, Article 8 of the European Convention on Human Rights and Article 14 of the African Charter on Human and Peoples' Rights.

748. The scope of the right to privacy is therefore incapable of definition, and may be described as a bundle or continuum of rights which have a variety of justification. The Indian Supreme Court in **Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others Writ Petition (Civil) No. 494 of 2012** summarised the holdings in various Court decisions on the right to privacy, and expounded on the scope and aspects of the right to privacy, including the protection of informational privacy as follows in paragraph 232 :

(i) *"privacy has always been a natural right, and the correct position has been established by a number of judgments starting from Gobind. Privacy is a concomitant of the right of the individual to exercise control over his or her personality. Equally, privacy is the necessary condition precedent to the enjoyment of any of the guarantees in Part III. The fundamental right to privacy would cover at least three aspects (i) intrusion with an individuals physical body, (ii) informational privacy and (iii) privacy of choice. Further, one aspect of privacy is the right to control the dissemination of personal information. Every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control commercial use of his/her identity.*

(ii) *The sanctity of privacy lies in its functional relationship with dignity. Privacy ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusions. While the legitimate expectation of privacy may vary from intimate zone to the private zone and from the private to the public arena, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy is a postulate of dignity itself. Privacy concerns arise when the State seeks to intrude into the body and the mind of the citizen.*

(iii) *Privacy as intrinsic to freedom, liberty and dignity. The right to privacy is inherent to the liberties guaranteed by Part-III of the Constitution and privacy is an element of human dignity. The fundamental right to privacy derives from Part-III of the Constitution and recognition of this right does not require a constitutional amendment. Privacy is more than merely a derivative constitutional right. It is the necessary basis of rights guaranteed in the text of the Constitution.*

(iv) Privacy has both positive and negative content. The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual.

(v) Informational Privacy is a facet of right to privacy. The old adage that knowledge is power has stark implications for the position of individual where data is ubiquitous, an all-encompassing presence. Every transaction of an individual user leaves electronic tracks, without her knowledge. Individually these information silos may seem inconsequential. In aggregation, information provides a picture of the beings. The challenges which big data poses to privacy emanate from both State and non-State entities.

(vi) Right to privacy cannot be impinged without a just, fair and reasonable law. It has to fulfil the test of proportionality i.e. (i) existence of a law (ii) must serve a legitimate State aim and (iii) proportionate.

749. The protection of informational privacy is what is specifically in issue in the instant Petition, and is provided for in Article 31 (c) of the Constitution. The scope of the right to and protection of informational privacy is explained in **The Bill of Rights Handbook, 5th Edition (2005)** by Iain Currie and John de Waal at page 323, as follows:

“More particularly, this is an interest in restricting the collection, use and disclosure of private information. It also encompasses a related interest in having access to personal information that has been collected by others in order to ascertain its content and to check its accuracy. These interests can readily be accommodated under the value of dignity since publication of embarrassing information, or information which places a person in false light, is most often damaging to the dignity of the person. But the right to privacy guarantees control over all private information and it does not matter whether the information is potentially damaging to a person’s dignity or not. The publication of private photographs, however flattering, will for example constitute a violation of the right to privacy of in this sense. So would be the use of a person’s name or identity without his or her consent. But as with the other two elements of the right to privacy, there must be a reasonable expectation of privacy. For example, a person does not have the right to refuse to provide identification to a police official when so requested.”

750. Information privacy includes the rights of control a person has over personal information. Such personal information will in the first place concern information which closely relates to the person and is regarded as intimate, and which a person would want to restrict the collection, use and circulation thereof. Examples include information about one’s health. But other information about that person may also be considered ‘private’ and hence protected under the right to information privacy, even if this information relates to his or her presence or actions in a public place or a place accessible for the public. Such information over which individuals have an interest to keep private in our view also include information and data about their unique human characteristics, which allows them to be recognized or

identified by others, as it is information about one's body and about one's presence, image and identity, in both private and public places.

751. We accordingly adopt the definition in **Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others (supra)**, where Lenaola J. and Muriithi J. summarised the right to informational privacy as follows:

“Article 31(c) of the Constitution must be understood in this context – it protects against the unnecessary revelation of information relating to family or private affairs of an individual. Private affairs are those matters whose disclosure will cause mental distress and injury to a person and there is thus need to keep such information confidential. Taken in that context, the right to privacy protects the very core of the personal sphere of an individual and basically envisages the right to live one's own life with minimum interference. The right also restricts the collection, use of and disclosure of private information.

752. In light of the different facets and bases for the right to privacy, the applicable test in determining whether there is an invasion or violation of the right was laid down in **Bernstein vs Bester NO** (supra) as follows:

“It essentially involves an assessment as to whether the invasion is unlawful. And, as with other forms of anuria, the presence of a ground of justification (such as statutory authority) means that an invasion of privacy is not wrongful. Under the Constitution, by contrast, a two-stage analysis must be employed in deciding whether there is a violation of the right to privacy. First the scope of the right must be assessed to determine whether law or conduct has infringed the right. If there has been an infringement it must be determined whether it is justifiable under the limitation clause”.

753. Specifically as regards a determination of whether there is a violation of the right to informational privacy, the Constitutional Court of South Africa in the case of **Mistry v Interim National Medical and Dental Council of South Africa (1998) (4) SA 1127 (CC)** stated that the Court ought to take into account the fact; (i) whether the information was obtained in an intrusive manner, (ii) whether it was about intimate aspects of an applicants' personal life; (iii) whether it involved data provided by an applicant for one purpose which was then used for another purpose and (iv) whether it was disseminated to the press or the general public or persons from whom an applicant could reasonably expect that such private information would be withheld.

754. In the present Petition, the Petitioners have alleged that the amendments to the Registration of Persons Act violates the right to privacy as it seeks to introduce the collection of biometric data, which is sensitive personal data and is intrusive. Particular mention was in this regard made of the collection of DNA, which the Petitioners claim can not only be used to reveal and profile a person's genetic, health and other physical characteristics, but also that of their relatives. Also challenged was the requirement to provide Global Positioning System (GPS) co-ordinates, which the Petitioners claim can be used to track and conduct mass surveillance on the people in Kenya.

755. The Respondents did not dispute that biometric data in digital form will be collected in NIIMS, and argued that such biometric data is in any event already being collected in existing

identification and registration databases, and was allowed by section 5(1)(j) of the Act which allowed the Principal Registrar to keep any other particulars about the identity of a person. The Respondents specifically denied that DNA and GPS coordinates data will be, or was collected in NIIMS. The Respondents however did point out and explain why DNA data and GPS co-ordinates is necessary for identification.

756. In normal parlance, biometric data is any physical, biological, physiological or behavioral data, derived from human subjects, which has the potential to identify an individual. Biometric data identifies an individual through one or more unique factors specific to the physical identity of a person. It is in this regard not in dispute that section 3 of the Registration of Persons Act was amended by the impugned Act to include a definition of “biometric” as “unique identifiers or attributes, including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid (DNA) in digital form” It also introduces a definition of Global Positioning Systems (GPS) coordinates to mean “unique identifier of precise geographical location on the earth, expressed in alphanumeric character being a combination of latitude and longitude”.

757. In addition section 5 (1)(g) of the Act was also amended to include GPS coordinates as part of the information to be provided on place of residence, and a new paragraph 5 (1)(ha) inserted that provides for biometric data to be kept in the register of all persons in Kenya by the Principal Registrar. Lastly, a new section 9A was included, which is the one that establishes NIIMS which will inter alia harmonise, incorporate and collate data relating to registration of persons from all registers, including biometric data.

758. We start our analysis by addressing the legitimacy of the privacy concerns raised by the Petitioners about biometric data. The first observation we make in this regard is that biometric data, by its very nature, provides information about a given person, and is therefore in this regard personal information that is subject to the protection of privacy in Article 3. The Data Protection Act No. 24 of 2019 has adopted at section 2 the definition of personal data that is in the European Union’s General Data Protection Regulations (GDPR) and in the African Union Convention on Cyber Security and Personal Data Protection, namely, any information which is related to an identified or identifiable natural person.

759. The GDPR details the elements of such information as follows in Article 4(1);

“The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data”.

760. A similar definition of an identifiable natural person is now provided for in the Data Protection Act No. 24 of 2019. We note that the unique attributes and identifiers that are included in the definition of biometric data as defined in section 3 of the Registration of Persons Act, GPS coordinates, and the data collected by NIIMS as evidenced by the NIIMS Data Capture Form, clearly fall within the above definition of personal data. The qualification of biometric data as personal has important consequences in relation to the protection and

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 147 of 205.

processing of such data, and as such invites a risk of violation of the right to privacy in the event of inadequate protection measures.

761. The Petitioners also urged that the amendments introducing biometric data allow collection of sensitive data about persons. The concept of sensitive data has its origin in the European Union jurisprudence on the right to privacy and data protection, and the GDPR also recognizes that in addition to general personal data, there are special categories of personal data, known as sensitive personal data, which are subject to a higher level of protection. Similar provisions on sensitive data are provided in Article 1 of the African Union Convention on Cyber Security and Personal Data Protection. The Data Protection Act No. 24 of 2019 likewise defines sensitive personal data as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details including names of the person's children, parents, spouse or spouses, sex or sexual orientation of the data subject.

762. We note that such data is considered sensitive data because of the more serious impact of its loss or unauthorized disclosure, particularly in terms of the attendant social, reputational, or legal risks and consequences. It is thus evident that biometric data and in particular DNA must be protected against unauthorized access, and access to such data should also be limited through sufficient [data security](#) practices designed to prevent unauthorized disclosure and [data breaches](#).

763. The last allegation by the Petitioners was that biometric data and personal information being collected as a result of the impugned amendments is intrusive. Intrusion is defined in **Black's Law Dictionary, Ninth Edition** at page 900 as "*a person entering without permission*". Therefore, personal data is intrusive when it is collected without a person's knowledge of consent.

764. The Respondents testified in this regard that the data collected by NIIMS was with the consent of the subjects, while the Petitioners have contended that data collection was mandatory, and as such there was no informed consent. The Respondents brought evidence of the Data Capture Form used during the collection of the biometric data, which had a caption on the consent of the data subject, and also testified that they had removed the statement in the said Form that registration would be mandatory, in compliance with this Court's orders. The Petitioners did not bring any evidence of any person who was forced to give the consent, or did not understand the nature of the consent being given. In addition, this Court in its ruling delivered on 1st April 2019 had directed that the collection of the data would not be mandatory.

765. We however observe that at the time of the said data collection, there was no legal requirement for consent to be given by a data subject to the collection of biometric data. The Data Protection Act 24 of 2019 which has since been enacted now specifically provides for the rights of the data subject, including the right to object to the processing of his or her personal data in section 26 thereof. The Act also further provides in section 30(1) that the data subject must consent to processing of his or her personal data. We are therefore constrained to find that the data collection exercise undertaken pursuant to the impugned amendments was done with the consent of the data subjects.

766. As to whether the categories of personal data that will be collected pursuant to the impugned amendments is in their nature intrusive, this Court is guided by the observations in the **Working Document on Biometrics P 80** by the Article 29 Data Protection Working Petition 56, 58 & 59 of 2019 (Consolidated) | Page 148 of 205.

Party, which was an independent European Union Advisory Body on Data Protection and Privacy established pursuant to Article 29 of the then EU Directive 95/46/EC. The working Group stated as follows in the said Working Document, which it adopted on 1st August 2003:

“A further point which is crucial from a data protection point of view is the fact that some biometric systems are based on information, like fingerprints or DNA samples, that may be collected without the data subject being aware of it since he or she may unknowingly leave traces. In applying a biometric algorithm to the fingerprint found on a glass, one may be able to find out if the person is on file in a database containing biometric data, and if so, who he is, by proceeding with a comparison of the two templates. This also applies to other biometric systems, such as those based on keystroke analysis or distance facial recognition, on account of the specific features of the technology involved. The problematic aspect is, on the one hand, that this data collection and processing may be performed without the knowledge of the data subject and on the other hand that regardless of their current reliability, these biometric technologies lend themselves to blanket utilisation on account of their 'low-level intrusiveness'. Therefore, it seems necessary to lay down specific safeguards in respect of them.”

767. These observations confirm the Petitioners’ concerns as raised as regards the intrusive nature of some of the biometric characteristics that are provided for in section 3 of the Registration of Persons Act, including DNA. Irrespective of the fact that there are legitimate uses of DNA in identification, as pointed out by the Respondents, we are mindful of the risks of indiscriminate collection of genetic information and other biometric identifiers which makes such information susceptible to extraneous use, including negative profiling of individuals for ulterior motives as observed by Dr. Malombe in his affidavit. He noted that this can be done by matching a DNA profile or other biometric characteristic that can be collected without a person’s knowledge or consent, and he gave the example of how a DNA profile from a coffee cup can be compared with a stored DNA profile or other biometric characteristic in the identification database, and provide details about an individual’s name and address, among other things, and can be used to profile the individual.

768. On the concerns raised on the privacy and surveillance risks posed by the requirement to give information on GPS co-ordinates, this Court takes judicial notice of the fact that the GPS technology is satellite-based and its usage has different aspects, and is more commonly used in cars and phone mobiles which help in determining directions and locations. The potential usage of such technology may include information from the providers of internet and telecommunication services that permits real-time tracking of the directions, speed and locations of monitors. The privacy implications and risks arising from the use of GPS monitors is that the said devices can be used to track and monitor people without their knowledge.

769. The U.S. Supreme Court addressed these risks and threats in a unanimous decision in **United States v. Antoine Jones** 565 US (2012), and ruled that law enforcement must obtain a warrant prior to attaching a GPS device to a suspect’s vehicle in order to monitor its movements. The issue before the Court was whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual’s vehicle, and subsequent use of that device to monitor the vehicle’s movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment. The Fourth Amendment provides in the relevant part that

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 149 of 205.

the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

770. Sotomayor J. in his concurring judgment observed that the Government had usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to Fourth Amendment protection, and held as follows in this regard:

“GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about familial, political, professional, religious, and sexual associations.....Disclosed in GPS data will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on The Government can store such records and efficiently mine them for information years into the future.... And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices”

771. Therefore, while Mr. Ochieng (the 5th Respondent’s witness), explained that the GPS co-ordinates in the impugned amendments are required only for purposes of digital identification of an individual’s geographical location, their potential uses are much more, and in the context of identification of persons possess a risk to privacy. There is need for more detailed and strict regulation on the use of GPS co-ordinates, to avoid abuse and misuse of the provisions in the impugned amendments.

772. The upshot of our findings in the foregoing is that biometric data and GPS coordinates required by the impugned amendments are personal, sensitive and intrusive data that requires protection. This Court prohibited the analysis and use of the personal data collected during NIIMS for this reason, and even though there was no evidence brought by the Petitioners of any violations of rights to privacy in this respect, this Court finds that the impugned amendments impose an obligations on the relevant Respondents to put in place measures to protect the personal data.

773. To this extent, the answer to the question as to whether there is threat of a violation to the right to privacy in the provision for collection of biometric data and GPS coordinates is dependent on the adequacy of the protection measures of the said data, and will await an examination of the existing legal framework on the protection of data.

774. It is also notable that in Article 31 (c) of the Constitution, a violation of the right to informational privacy occurs when personal information is unnecessarily required or revealed. Therefore, the outstanding question before us is whether the requirement of, and collection of biometric data was necessary or not. The Petitioners in this regard urged that the said biometric data was not necessary for reasons that its purpose was not stated, and was purpose free. Closely related to this argument was the averment by the Petitioners that there is unnecessary data that was collected under NIIMS that was not necessary for identification, such as information on agricultural activities and landholding.

775. The Petitioners also challenge the utility of the biometric data in identification. The Petitioners also challenge the utility of the biometric data in identification, and their expert witnesses testified to the challenges some sections of the population may face in enrolling or authenticating certain biometric features such as worn fingerprints, the possibilities of reaching false conclusions while relying on biometric data as it relies on probabilities, and there will thus be no deduplication of data.

776. The justification put forward by the Respondents for the collection of biometric data was that the right to privacy is not an absolute right, that biometric data is necessary as the most deterministic method of identification, and that reliable data is necessary for the State to provide services and security to its citizenry. The Respondents also urged that the biometric data being collected is necessary for the purpose of creating a digitized national population register as a single source of personal information on all Kenyan citizens and residents. Their expert witnesses gave detailed evidence on the NIIMS design as a multi-modal system that will ensure that the biometric data is deterministic.

777. We have considered and appreciate the detailed information and evidence given by the parties on the nature of biometric data, and its use in identification. We need to clarify two aspects of the relevance of this evidence at the outset. Firstly, it is evident from the various definitions of biometric data that its main utility is with regard to identification of a natural person. To this extent, biometric data is necessary for identification purposes. We in this respect adopt the findings of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others (*supra*) on the necessity of the different types of biometric data in identification as follows:

“251. Face Photographs for the purpose of identification are not covered by a reasonable expectation of privacy. Barring unpublished intimate photographs and photographs pertaining to confidential situations there will be no zone of privacy with respect to normal facial photographs meant for identification.

Face-photographs are given by people for driving license, passport, voter id, school admissions, examination admit cards, employment cards, enrolment in professions and even for entry in courts. In our daily lives we recognize each other by face which stands exposed to all, all the time. The face photograph by itself reveals no information.

252 There is no reasonable expectation of privacy with respect to fingerprint and iris scan as they are not dealing with the intimate or private sphere of the individual but are used solely for authentication. Iris scan is nothing but a photograph of the eye, taken in the same manner as a face photograph. Fingerprints and iris scans are not capable of revealing any personal information about the individual except for serving the purpose of identification. Fingerprints are largely used in biometric attendance, laptops and mobiles. Even when a privacy right exists on a fingerprint, it will be weak. Finger print and iris scan have been considered to be the most accurate and non-invasive mode of identifying an individual. They are taken for passports, visa and registration by the State and also used in mobile phones, laptops, lockers etc for private use. Biometrics are being used for unique identification in e passports by 120 countries.”

778. Therefore, the only relevant consideration as regards the necessity of biometric data is its utility with respect to the authentication or verification of a person. The Article 29 Data Protection Working Party in its **Working Document on Biometrics** identified the necessary qualities required of biometric data for purposes of authentication and verification are that the data should have attributes that are: (a) universal, in the sense that the biometric element exists in all persons; (b) unique, in that the biometric element must be distinctive to each person, and (c) permanent, in that the biometric element remains permanent over time for each person, and a data subject is in principle not able to change these characteristics.

779. It is notable in this respect that the biometric attributes required by the impugned amendments meet these criteria, as most of them are universal and unique to the data subjects. The only reservation we have is as regards the utility of DNA for identification purposes. This is for the reason that unlike other biometric characteristics, the technique used in DNA identification, which is a DNA comparison process, does not allow for the verification or identification to be done “in real time”, the comparison is also complex, requires expertise, and takes time.

780. The European Court of Human Rights in **S. and Marper v United Kingdom** **30562/04 [2008] ECHR 1581** addressed the issue of the utility of holding DNA in a database, and found that the continued holding of DNA samples of individuals who are arrested but later acquitted or have the charges against them dropped, is a violation of the right to privacy under the European Convention on Human Rights. Some of the reasons given by the Court as to why the retention of cellular samples and DNA profiles was a breach of the right to privacy were as follows:

“73. Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see Amann, cited above, § 69).

74. As regards DNA profiles themselves, the Court notes that they contain a more limited amount of personal information extracted from cellular samples in a coded form. The Government submitted that a DNA profile is nothing more than a sequence of numbers or a barcode containing information of a purely objective and irrefutable character and that the identification of a subject only occurs in case of a match with another profile in the database. They also submitted that, being in coded form, computer technology is required to render the information intelligible and that only a limited number of persons would be able to interpret the data in question.”

781. We find that the limitations observed by the Court in the said case on the use of DNA equally apply, if not with more potency, to the Kenyan situation, given the concession by the Respondents of their inability to process DNA information for the entire population. Lastly, we also find that the necessity of GPS monitors in identification is even less evident, given the risk they pose to the right to privacy as we found earlier on in this judgment, and the Respondent’s concession of its inability to collect this information.

782. It is also our view that the evidence by the Petitioners as regards the shortcomings of some of the biometric data in these respects is one that is material to the identification system designs to ensure that usability, reliability and effectiveness. As explained by the different experts who testified before us, the uniqueness of the characteristics captured by the NIIMS identification system will determine the effectiveness of biometric systems. The choice of one or more particular characteristics for a system will further be influenced by the acceptance of its use by the individuals, and may also influence the architecture of a biometric system. It however does not obviate the need or necessity for biometric data in identification. Therefore, for example, even though a biometric characteristic may be considered universal, for example a "ngerprint, it does not mean that all persons will have the required biometric characteristic. Persons may have lost a biometrically relevant characteristic through accident, sickness or peculiar circumstances. In such cases, more than one biometric characteristic of the same data subject are combined to improve performance.

783. We therefore are persuaded by the evidence of the experts called by the Respondents that the combination of two characteristics, for example more than two "ngerprints, or the use of more than one type of characteristics, such as face and voice, generally improves the performance of the system. We also found the evidence by the Respondents on the multi-modal nature of NIIMS relevant, to the extent that the system entails the collection of different types of biometric data to improve its deterministic nature. To this extent, we also find that the Respondents did demonstrate why the provision for, and collection of different types of biometric characteristics was necessary.

784. Accordingly, in light of our analysis in the preceding paragraphs of this judgment, our findings are that other than the DNA and GPS coordinates, information to be collected pursuant to the impugned amendments to the Registration of Persons Act is necessary and is therefore not unconstitutional. However, with regard to collection of DNA and GPS co-ordinates for purposes of identification, it is our finding that it is intrusive and unnecessary. To the extent, therefore, that it is not authorised and specifically anchored in empowering legislation, it is unconstitutional and a violation of Article 31 of the Constitution.

785. On the last aspect raised as regards the purpose of the data collected in NIIMS, the Respondent testified that the purpose of collection of the biometric data was to create a digital database which they termed "a single source of truth" as regards the identity of persons in Kenya in the form of NIIMS. Reference was made to section 9A of the Registration of Persons Act on the establishment of and purposes of NIIMS. The said section provides for the functions of NIIMS as follows:

(a) 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;

(b) to assign a unique national identification number to every person registered in the register;

(c) to harmonise, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons;

(d) to support the printing and distribution for collection all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel

documentation, student identification cards issued under the Births and Death Registration Act, Basic Education Act, Registration of Persons Act, Refugees Act, Traffic Act and the Kenya Citizenship and Immigration Act and all other forms of government issued identification documentation as may be specified by gazette notice by the Cabinet Secretary;

(e) to prescribe, in consultation with the various relevant issuing authorities, a format of identification document to capture the various forms of information contained in the identification documents in paragraph (d) for purposes of issuance of a single document where applicable;

(f) to verify and authenticate information relating to the registration and identification of persons;

(g) to collate information obtained under this Act and reproduce it as may be required, from time to time;

(h) to ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register;

(h) to correct errors in registration details, if so required by a person or on its own initiative,

(i) to ensure that the information is accurate, complete, up to date and not misleading; and

(j) to perform such other duties which are necessary or expedient for the discharge of functions under this Act.

786. Some of the stated purposes of NIIMS under section 9A are the creation of a national population register, the assigning of a unique identification number to every person registered in the register, and the verification and authentication of information on the identity of persons. It is thus principally an identification and verification system. These two functionalities are explained in the text on **Privacy and Data Protection Issues of Biometric Applications**, by Els Kindt (2003) in paragraphs 85 to 88, wherein it is opined that the identification function recognizes an individual by comparing the submitted biometric characteristic with all previously submitted and stored biometric characteristic in one or more databases through a search. Further, that the verification is possible with a comparison of one submitted set of characteristics with a pre-defined and pre-stored set of characteristics.

787. Therefore, the identification and verification functionalities will always need the existence of a database with the biometric data stored for comparison. Such storage can be done centrally, for example in a central database, but it is also possible to store the biometric data for comparison locally, for example on an object which the data subject holds and which remains in his or her possession. In addition, the verification and identification functionalities may also be combined in one system. To this extent, the biometric data collected is necessary to the stated purposes of NIIMS as is clear that the system can only provide trustworthy information about the identity of the person if the characteristics of that person are stored in its database.

788. These functionalities in our view also explain the utility of NIIMS and the other existing identification and registration databases that was urged by both the Petitioners and Respondents. It is thus our finding that NIIMS is not superfluous from an identification and

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 154 of 205.

verification point of view, as the biometric data collected therein is necessary for identification, and will be used for verification purposes in relation to other existing databases.

789. As regards the other data that was collected during the NIIMS registration, additional stated purposes of NIIMS in section 9A are that of harmonizing and collating of data information from other databases in Government agencies relating to registration of persons and also prescribing consultation on the issuance of identification documents. The Respondents testified that the collection of the additional data was decided and agreed upon by the concerned Government agencies in the Inter-Ministerial Committee implementing NIIMS arising from the need for the data, and for the Government to be cost effective but also for efficiency reasons. We find this explanation to be reasonable, and given that such cooperation with other agencies in registration of persons is also allowed by the law, we do not find the data so collected to be unnecessary.

790. In conclusion, it seems to us that the Petitioners' concerns in this respect conflated the stated purpose of NIIMS as provided in the law, with the veracity of its benefits as alleged by the Respondents. As held in **R vs Big M Drug Mart Ltd** (*supra*) both the purpose and effect of a legislation are relevant in determining the constitutionality of a legislation. In this regard the Respondents have demonstrated that the purpose of the impugned legislation is to set up an identification system, and to the extent that it is necessary, then the same is constitutional. On the other hand, the Petitioners did not demonstrate in what manner the benefits are unconstitutional, and instead seemed to demand evidence of their existence, and the ranking of their priority and importance. It is our view and finding that the stated benefits of NIIMS given by the Respondents in their evidence are in the public interest and not unconstitutional.

Whether there is a Violation of Children's' Rights to Privacy

791. An additional limb of the challenge to the NIIMS process with respect to its alleged violation of the rights to privacy relates to the rights of privacy of children. The Petitioners and the Interested Parties who support them argue that while the impugned amendments and the resultant process of digitisation of data applies to everyone, including children, section 2 of the Act does not include children. It is their argument that by providing that it applies to persons over the age of 18 years, it specifically excludes the application of its provisions to children.

792. In its submissions, the 2nd Petitioner notes that one of the reasons advanced for NIIMS is that it was discovered that information relating to children was not being captured comprehensively at birth. The government was accordingly keen to achieve 100% registration of births, and one of the ways it intended to do so was by employing suitable technology. The 2nd Petitioner argues, however, that section 2 of the Act applies the Act exclusively to persons who are citizens of Kenya and who have attained the age of eighteen years or over or, where no proof of age exists, are of the apparent age of eighteen years or over. It submits that though the impugned amendments purport to apply the Act to all persons, the limitation under section 2 is a patent defect that renders the Act vague and, accordingly, defective. It was also its submission that for the above reasons, its application to children is unreasonable, unjustifiable and unnecessary.

793. According to the 2nd Petitioner, section 9A(2) of the Act establishes a very generic, wide and ambiguous scope of the functions of NIIMS. It further notes that there are essentially no restrictions with regard to what the personal data collected, including children's personal data, Petition 56, 58 & 59 of 2019 (Consolidated) | Page 155 of 205.

may be used for. It is its submission that given children's vulnerable status, clear distinctions should have been prescribed for collection, use, processing and storage of children's data relative to adults.

794. The 2nd Petitioner notes that under the impugned amendments, parents have a mandatory duty to surrender their children's information failing which they face the threat of criminal sanctions which is contrary to international laws, best practices and standards. It was its view that there was no problem or challenge so grave that required mandatory registration of children backed by criminal sanctions. The 2nd Petitioner relies on the decision in the **Julian Robinson Case** for the proposition that difficulty in establishing identification is not a synonym for an inability to establish identity.

795. The 5th Interested Party, echoes the submissions of the 2nd Petitioner with regard to the application of section 2 of the Act. It submits that the section only applies to citizens of Kenya who have attained the age of 18 years, not to children or foreign nationals. It notes that in the training manual produced as evidence by Dr. (Eng) Karanja Kibicho the registration assistants were given express instructions to collect personal information on children. It is its submission that the collection of personal information on children and non-citizens is *ultra vires* section 2 of the Act.

796. With respect to the contention by the Respondents that the collection and digitisation of children's data will help in combating child labour and child trafficking, the 5th Interested Party argues that this will not in fact be the case, that the use of biometrics does not help in the protection of children and only creates their digital identity earlier than is necessary.

797. In its response to the arguments on this issue, the 1st Respondent contends that from a national security perspective, NIIMS would play an indispensably crucial role in obviating and combating contemporary crimes such as terrorism, child labour and trafficking in children, and would aid in keeping the country safe from terrorist attacks.

798. In their submissions in response, the 2nd and 3rd Respondents note the constitutional requirement under Article 53 that a child's best interests shall be the primary consideration in any matter concerning the child. They further submit that the implementation of NIIMS is in the best interests of children. This is because it enables the State to fulfil its constitutional obligations to children, which include the obligation to protect and promote children's right to free and compulsory basic education, basic nutrition, shelter and healthcare, as well as the obligation to be protected from abuse, neglect, harmful cultural practices, all forms of violence, inhuman treatment and punishment, and hazardous or exploitative labour in accordance with Article 53 of the Constitution.

799. The 2nd and 3rd Respondents further note that the constitutional obligations are also provided for in international instruments ratified by Kenya, among them Article 8(1) of the 1989 United Nations Convention on the Rights of the Child and Article 24(1) of the 1966 International Covenant on Civil and Political Rights. The 2nd and 3rd Respondents submit that the non-existence of a mechanism for uniquely identifying children has prevented the government from meeting its obligations under the Constitution and international covenants. It is their submission that birth certificates which act as the only contemporary legal means of identification of children are solely distinguished by use of serial numbers and do not bear a child's fingerprints, facial image or any other biometric. They argue that as a result, criminal elements have capitalized on the limitations of a birth certificate to perpetuate child

trafficking and child labour and other child-related offences. In their view, NIIMS would cure the mischief that is attributable to the current child identification system.

800. The 2nd and 3rd Respondents term the allegation that NIIMS would violate children rights due to the absence of mechanism for correcting and updating inaccurate information on children's data unfounded. It is their submission that the legislative provisions impugned by the Consolidated Petitions provide for corrective measures. They cite in this regard section 9A(2) (i) of the Act which empowers NIIMS to correct errors in registration details, if so required by a person or on its own initiative in order to ensure that the information in the system is "*accurate, complete, up to date and not misleading.*" They submit that parents and guardians of children may therefore, correct and update the identity information of the children for whom they are responsible.

801. The 2nd and 3rd Respondents submit that as demonstrated by the NIIMS data capture form, the children data to be stored under NIIMS would be limited to registration and identity data. They assert that the principle of data minimization was adopted in the design architecture of NIIMS in the sense that any information that may be incorporated into the NIIMS database from databases of other government agencies would be limited to information on registration of persons, citing in this regard section 9A(2) (c) of the Act.

802. The 2nd and 3rd Respondents assert that the fear of threat of constant surveillance of children is unfounded. It is their case that they have demonstrated that functional data will remain resident in their respective functional databases as maintained by various ministries, departments and agencies. In their view, in the unlikely event that the NIIMS database was to be compromised, the functional data of children such as academic and health records will be unaffected.

803. The 2nd and 3rd Respondents contend that the 2nd Petitioner's claim that the collection of DNA identity data is too intrusive and would violate the privacy of data subjects is baseless. They submit that the collection and processing of DNA is generally permissible in this country. They rely in support on the decision in **L.N.W. v. Attorney General & 3 Others [2016] eKLR** in which it was held that changes should be made in the law to allow for the names of fathers of children born outside marriage to be entered in the births register and the children's birth certificates, and that provision should also be made for DNA testing to be undertaken to establish paternity should paternity be denied. It is their submission that the decision in **L.N.W v Attorney General & 3 others (supra)** was an affirmation by the Court that DNA testing of children is permissible for purposes of the realization of the right of children to know their parents. In their view, it followed that the collection of DNA would be permissible for the attainment of other rights, more so where such rights are crucial to the life and security of children.

804. The 2nd and 3rd Respondents further submit that the collection of DNA is in certain circumstances a crucial form of identification. This is particularly so where there are no other personal identifiers. They cite in this regard cases of fatal flight accidents where all other components of an individual's biometrics are destroyed, leaving the use of DNA as the only way of identifying the remains. It is also their submission that DNA evidence is also a crucial part of the law of evidence in resolving certain crimes such as rape, murder or manslaughter.

805. The 2nd and 3rd Respondents observe that the data privacy concerns in relation to children raised by the 2nd Petitioner have been grounded on the European Union's General Data Protection Regulation (GDPR). It is their submission that the GDPR are European Union Petition 56, 58 & 59 of 2019 (Consolidated) | Page 157 of 205.

law and have no binding effect in Kenya. Further, that the principles espoused in the GDPR have not attained the status of universal applicability, having entered into force on 25th May 2018.

806. It is their submission, however, that in the event that this court finds that the GDPR is binding on Kenya, they would invoke Article 86 of GDPR which gives the Member States the discretion to determine the specific conditions for the processing of a national identification number or any other identifier of general application. It is their case that this provision acknowledges the legitimacy of the use of a national identification number and the lawfulness of processing of personal information for purposes of generating the said national identification number.

807. The 2nd and 3rd Respondents further note that recital 46 of GDPR renders lawful the processing of personal data where such processing is necessary to protect an interest essential for the life of the data subject or of another natural person. It is their case that some types of processing may serve both important grounds of public interest and the vital interests of the data subject. Such situations in which processing is necessary for humanitarian purposes include for monitoring epidemics and their spread and humanitarian emergencies such as in situations of natural and man-made disasters.

808. The 2nd and 3rd Respondents therefore submit that the existence of an efficient and organized system of registration and identification of individuals coupled with responsible use of public resources in the process justifies the processing of personal information under NIIMS.

809. The reasons advanced by the Respondents for the registration of children into NIIMS sound reasonable and laudable. They include national security concerns such as the need to combat terrorism, the need to enable the State to fulfil its obligations to children under Article 53 of the Constitution, deal with the inadequacies presented by the birth certificate as an identifier for children in light of the fact that it only has a serial number and does not have children's biometric data and is therefore not suitable as a means to combat child trafficking and child labour. To this extent we cannot find the impugned amendments' effect on children unconstitutional.

810. The Respondents have not, however, addressed the core issues that we believe the Petitioners' objection to the collection of children's data are hinged upon: that the Act does not apply to children, the collection and security of their biometric data, and the criminalisation of failure by a parent or guardian to register a child with NIIMS. While the Respondents argue that one of the reasons for NIIMS is that the government had discovered that information relating to children was not being captured comprehensively at birth and NIIMS was intended to assist the government achieve 100% registration of births through the use of technology, they have elected to anchor the system under which they intend to collect children's data on legislation that expressly excludes children. Enacted in 1949, the Act's long title indicates that it is an "*Act of Parliament to make provision for the registration of persons and for the issue of identity cards, and for purposes connected therewith.*"

811. Section 2 of the Registration of Persons Act provides as follows:

This Act shall apply to all persons who are citizens of Kenya and who have attained the age of eighteen years or over or where no proof age exists, are of the apparent age of eighteen years or over.

812. The Petitioners are thus correct in their contention that the Act does not apply to children and persons who are not citizens of Kenya. Section 9A which was introduced by the impugned amendments, however establishes the NIIMS system, and provides that one of its functions is to create a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya. It does not make any exception for children. The question is what is the effect, with respect to collection of children's data, of anchoring NIIMS in legislation that specifically excludes children" The Petitioners argue that this renders the Act vague and defective, and its application to children unreasonable, unjustifiable and unnecessary.

813. It appears to us that the manner in which NIIMS was brought into being does not reflect much thought on the part of the Respondents. While from the Respondents' evidence it is clear that NIIMS is intended for all citizens and foreigners' resident in Kenya, it was however provided for in legislation providing for registration and issuance of identification documents for adults who are citizens of Kenya. We note that in response to the contention that there are inconsistencies between NIIMS and other registration institutions and systems such as IPRS, the 2nd and 3rd Respondents argue that where appropriate, NIIMS would be deemed to override any earlier statutory provision that is inconsistent with it. Reliance is placed for this contention on the authority of **Kenya Pharmaceutical Distributors Association v Kenya Veterinary Board & 3 others** [2017]eKLR where the Court held that the provisions of the Veterinary Surgeons and Veterinary Para-Professionals Act, being of a latter statute, override those of the Pharmacy and Poisons Act where appropriate. The Court was guided in its decision by what it referred to as the settled principle that "*a latter provision or statute overrides the older one or is deemed to have repealed the earlier one.*"

814. The question before us is whether this reasoning is applicable in respect of a latter amendment to a statute that conflicts with an earlier provision with respect to the application of the Act. To find a solution to this conflict, we can only seek guidance from the principle of statutory construction and interpretation. The rules of statutory interpretation of relevance in this respect are those on implied amendment and implied repeal. These rules provide that where a later enactment does not expressly amend (whether textually or indirectly) an earlier enactment which it has power to override, but the provisions of the later enactment are inconsistent with those of the earlier, the later by implication amends the earlier so far as is necessary to remove the inconsistency between them. If the later Act cannot stand with an earlier, Parliament is taken to intend an amendment of the earlier.

815. This is a logical necessity, since two inconsistent texts cannot both be valid without contravening the principles of contradiction, that is, contradictory statements cannot both at the same time be true and the court must do its best to reconcile them. If the entirety of an earlier Act is inconsistent, the effect amounts to a repeal of it. The test to applied to determine whether there has been a repeal by implication by subsequent legislation is whether the provisions of a later Act are so inconsistent with, or repugnant to, the provisions of an earlier Act that the two cannot stand together, as stated by A.L. Smith J. in **West Harm Church Wardens and Overseers v Fourth City Mutual Building Society** (1892) 1 QB 654 at 658. Also see the detailed explanations in this respect in **Francis Bennion on Statutory Interpretation**, 3rd Edition, pg 214-226, and the decisions in **Martin Wanderi & 19 others vs EngineersRegistration Board of Kenya & 5 others** (2014) eKLR and **AO O & 6 others v Attorney General & another** [2017] eKLR.

816. Applying these principles to the present Petition, it is evident that the provisions of section 9A of the Registration of Persons Act on the purposes of NIIMS contradicts section 2, and the two provisions cannot operate at the same time with regards to the application of NIIMS to children. After applying the rules of statutory interpretation on implied amendment and repeal detailed out in the foregoing, it is our finding section 9A being a later amendment is deemed to have amended section 2 with respect to its application to NIIMS, and to this extent the inconsistency is thereby resolved. We therefore find that section 9A of the Registration of Persons Act and NIIMS applies to children.

817. A second concern raised by the Petitioners with respect to the collection of children's data is that the amendments set out in section 9A(2) of the Act establish NIIMS and vest in it functions that are very generic, wide and ambiguous in scope; that there are no restrictions with respect to what the personal data collected, including children's personal data, may be used for. In its view, given children's vulnerable status, clear distinctions should have been prescribed, distinct from those made regarding data collected from adults, with respect to the collection, use, processing and storage of children's data. This contention ties in with the concerns raised in the affidavit and oral evidence of Ms. Grace Bomu Mutung'u. While Ms. Mutung'u's expertise with respect to children's data was exposed, particularly in the cross-examination by Mr. Regeru, as rather limited, one cannot fault the principles she presented to court with regard to children, relative to adults.

818. The 2nd Petitioner also submitted that under the impugned amendments, parents have a mandatory duty to surrender their children's information failing which they face the threat of criminal sanctions which is contrary to international laws, best practice and standards. It was its view that there was no problem or challenge so grave that requires mandatory registration of children backed by criminal sanctions.

819. We start our analysis on the concerns raised as regards the protection of children's personal data and privacy by clarifying that there is no specific provision in the impugned amendments that provide for criminal sanctions for parents of children, as alleged by the 2nd Petitioner, and the 2nd Petitioner did not point us to any such amendment. The only effect of the impugned amendments that establish NIIMS in this regard is to extend the application of the Act to children, which we have already addressed in the foregoing.

820. Having made that clarification, we are of the view and find that the general principles and protections that apply with regards to the right to informational privacy, and our findings in this regard with respect to the biometric data collected under NIIMS, are also applicable to children as much as they apply to adults, and perhaps even more. This is because unlike adults, children's ability to make reasonable choices about what information to share is limited, as a result of their limited capacities, development and education, and they may thus be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. In addition, we are also of the view that while digital literacy may be considered a dimension of the rights of children to freedom of expression, participation and education, the digital environment can also exposes children to harmful content, as well as privacy and data protection risks.

821. The question that therefore arises is whether the impugned amendments and NIIMS provide specific protection with regard to children's personal data, in light of the above-stated realities. In this regard, there is need for particular conditions that will apply to a child's consent to process personal data, which clearly indicate the age when a child is capable of

giving such an informed consent, and the requirement of informing the child in an appropriate manner of the implications of such consent. In addition, where a child is not capable of giving such consent, the consent must be given or authorised by the verified holder of parental responsibility over the child. The status of the data given by a child upon attaining the age of majority and the rights to that data also needs to be addressed by legislation, particularly where the data subject gives his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data.

822. We note that no such special protection was provided with respect to the biometric data collected from children under the impugned amendments, and there is clearly a risk of violation to children's right as a result of this inadequacy. We however note that the Data Protection Act No. 24 of 2019 now provides for the processing of personal data relating to a child under section 33 as follows:

“(1) Every data controller or data processor shall not process personal data relating to a child unless—

(a) consent is given by the child’s parent or guardian; and

(b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of—

(a) available technology;

(b) volume of personal data processed;

(c) proportion of such personal data likely to be that of a child;

(d) possibility of harm to a child arising out of processing of personal data; and

(e) such other factors as may be specified by the

(f) Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).”

823. We have noted some gaps in the said provisions, namely that there is no definition of a child in the Act, and the rights of the child in relation to the personal data collected during minority and upon attaining majority are also not specified, particularly in light of their evolving capacities. In addition, as observed earlier, despite NIIMS being applicable to children, there are no special provisions in the impugned amendments, and no regulations that govern how the data relating to children is to be collected, processed and stored in NIIMS. It is thus our finding that the legislative framework on the protection of children's biometric data collected in NIIMS is inadequate, and needs to be specifically provided for.

Whether there are Sufficient Legal Safeguards and Data Protection Frameworks

824. This issue was similarly argued from several fronts by the parties. The first front presented by the Petitioners was that there are insufficient data protection laws to secure the personal information collected in NIIMS. The 1st Petitioner submits that the impugned amendments incorporate a broad, non-exhaustive, definition of “biometric”, however, that there are no laws in place for the protection of such sensitive data to be collected by the Respondents. Moreover, that the amendment does not provide with precision the persons that shall have access to the sensitive data collected and with what persons the data can be shared.

825. The 1st Petitioner further argues that the laws in place such as the Access to Information Act and Computer Misuse and Cybercrimes Act were not enacted to implement Article 31 of the Constitution. It was contended that the effect of such a void in the law is that the data could fall in the hands of unauthorized third parties which is a contravention of the right to privacy and no one shall take responsibility for the damages suffered.

826. The 2nd Petitioner’s submissions were that the impugned amendments sanction mandatory or non-consensual collection of personal information without concomitant data protection laws. Further, that the data protection laws legislate and operationalize key data protection principles that strike the balance between the use of information and communication technologies and the protection of the privacy of citizens. The said principles of data protection were detailed by the 2nd Petitioner. It was its submission that contrary to international standards and best practices that advocate for the clear and explicit regulation of the entire spectrum of data collection, retrieval, processing, storage, use and disclosure, the impugned amendments appear to place a premium on what the Government believes will make its work easier with least or no regard whatsoever to the effect of its actions on privacy rights.

827. Furthermore, that the Principal Secretary in the Interior Ministry has been given free rein to prescribe subsidiary regulations on critical aspects of personal data, which should otherwise be regulated by a substantive data protection law, which is in breach of Article 94(6) of the Constitution which provides for conditions that apply when regulation making power is given to any public officer.

828. The 2nd Petitioner further submits that the risks of the foregoing weaknesses of NIIMS are further exacerbated by the absolute lack of data protection laws for the sensitive personal biometric data proposed for collection under the impugned amendments. In its view, the conceptualization of NIIMS and its operationalization contravene every known data protection law, rule, standard, policy and best practices, most of which were adduced as evidence by the Respondents, including the Data Protection Policy and Bill of 2019 and the EU GDPR .

829. In conclusion, the 2nd Petitioner submits that criminal sanctions cannot be sufficient safeguards to mitigate against the risks of data misuse and privacy breaches. Further, that by its very nature, technology is borderless and can be breached from anywhere including overseas. Accordingly, for the operationalization of NIIMS to give effect to the right to privacy under Article 31, it is imperative that appropriate technical and legal standards be formulated to ensure the security of the proposed digital identification system and the privacy of personal data collected by the same, and that no prejudice will be occasioned to any person in suspending the impugned laws until then.

830. The submissions by the 3rd Petitioner were that there is no data protection law or policy in place that would adequately address the concerns in the event there is misuse of information, and yet Article 24 of the Constitution sets out clear, concrete and objective circumstances in which a right or fundamental freedom in the Bill of Rights may be limited.

831. The 5th Interested Party joins the Petitioners in reiterating that the law under which all the activities under NIIMS are purported to be done, including collection of personal information, lacks the safeguards required of a law that authorizes the processing of personal information. It relied on the **Julian Robinson Case** where the Supreme Court of Jamaica directed that the law must afford appropriate safeguards to prevent use of the data in a manner inconsistent with the guaranteed right. Further, that the GDPR also prohibits the processing of biometric information, which may only be allowed where the data subject has given explicit consent and in specified circumstances, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. It was also pointed out that these standards are replicated in the African Union Convention on Cyber Security and Personal Data Protection, which is evidence that data protection standards may be elevated to the level of a general rule of an international law, making it a valid source of law in Kenya.

832. The Respondents in their submissions sought to illustrate that there were sufficient data protection laws. The 1st Respondent submits that there are ample statutory and regulatory safeguards for data protection, and that active steps are being taken to make the said safeguards even more robust. To that end, that section 28 of Access to Information Act 2016 makes provisions for the punishment of three years imprisonment or a fine not exceeding 1 million or both to any person who knowingly discloses exempt information, including information that entails unwarranted invasion of the privacy of an individual. It was its submission further, that the Kenya Information and Communication Act No. 2 of 1998, and Computer Misuse and Cybercrimes Act No.5 of 2018 provide additional protection that enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes.

833. In this respect, it was contended that NIIMS as introduced by the impugned amendment is a “protected computer system” which by definition means a computer system used directly in connection with, or necessary for the provision of national registration systems. Further, that the penalty for any unlawful interference is enhanced to 25 million shillings or imprisonment of a term not exceeding twenty years or both. In view of the foregoing, the 1st Respondent submits that there exists legal and institutional framework for the promotion and protection of personal data.

834. The 2nd and 3rd Respondents urge that that the constitutionality of the subject amendments cannot be challenged on the basis of alleged absence of adequate data protection law. They based that submission on the reasoning of Chief Justice Sykes in the **Julian Robinson Case**, where he opined that “constitutionality or lack of it cannot be decided on what legislation is to come; and is determined on what is.” The said Respondents further relied on the case of **Bernard Murage v Fineserve Africa Limited & 3 others** [2015] eKLR, where the Court declined the invitation to halt the roll out of Thin SIM technology pending the enactment of the Data Protection Bill, and observed that it cannot order Parliament to make specific laws but only test both the process leading to those laws and their contents against the constitutional muster.

835. The 4th and 7th Respondents also submit that there are safeguards in place to ensure the security of the information through extensive legislative framework on data protection, information security, modalities on access to information as well as protection of the integrity of government records and information. Furthermore, that the Access to Information Act, 2016 contains safeguards for the protection of the data to be stored in NIIMS, and provides that it is an offence for any person to disclose exempt information in contravention of the Act.

836. The above submissions were echoed by the 5th Respondent, who acknowledged that there is no exclusive data protection law, save for a data protection policy which is in operation. It was further its submission that there is a Data Protection Bill currently under debate in the National Assembly. That once passed, the Bill shall give effect to Article 31(c) of the Constitution, and shall also regulate the collection, retrieval, processing, storing, use and disclosure of personal data. In addition, the 5th Respondent submits that notwithstanding the lack of a specific data protection law, numerous statutes offer safeguards to State held data.

837. To that end reference was made to the Kenya Information and Communication Act (KICA) which provides for specific offences in this regard. The 5th Respondent further submits that the Official Secrets Act classifies government information and protect personal data and the Computer Misuses and Cyber Crimes Act 2018, provides for offences and penalties relating to computer systems. With particular respect to Registration of Persons Act, it was the 5th Respondent's submission that it has a limitation on who may access personal data and who can use it or share it. Furthermore, that there has been no previous breach of the data, that would have required an amendment to cater for NIIMS.

838. In light of the intervening events after the hearing of this case in terms of enactment of the Data Protection Act of 2019, we will address the arguments on the legal framework for data protection at this stage, before dealing with the other arguments made by the Petitioners on the adequacy of the safeguards for data protection. In this respect, when the parties were given an opportunity to submit on the Data Protection Act, all the parties requested the Court to take judicial notice of the Data Protection Act. There were however differing opinions as to how we should do so. The Petitioners were emphatic that we should take judicial notice of the passing of the Act and nothing more, while the Respondents submitted that taking judicial notice of the Act, entailed consideration of the Act's provisions.

839. Section 60 (1) of the Evidence Act obliges this Court to have judicial notice of all written laws, and provides as follows in this regard:

“60. (1) The courts shall take judicial notice of the following facts –

(a) all written laws, and all laws, rules and principles, written or unwritten, having the force of law, whether in force or having such force as aforesaid before, at or after the commencement of this Act, in any part of Kenya”

840. The role and effect of judicial notice is explained in Halsbury's Laws of England, Fourth Edition at paragraph 100 as a special mode of proving evidence, and it is stated therein that in addition to the adducing of documents and testimony of witnesses, the other modes of proving or establishing a fact are formal admissions, judicial notice, presumptions and inspection. Judicial notice is therefore a rule in the [law of evidence](#) that allows a fact to be introduced into evidence, if the truth of that fact is so notorious or well known, or so authoritatively attested, that it cannot reasonably be doubted.

841. Furthermore, facts and materials admitted under judicial notice are accepted without being formally introduced by a [witness](#) or other rule of evidence, and they are even admitted if one party wishes to lead evidence to the contrary. It is thus our opinion that we will not only take judicial notice of the fact that the Data Protection Act 24 of 2019 was enacted, but also of the law contained therein, as expressly provided by section 60 (1) of the Evidence Act. In this respect we note that the date of commencement of the Data Protection Act 24 of 2019 was 25th November 2019.

842. We have observed in our earlier findings that the protection of personal data depends largely on a legal, regulatory and institutional framework that provides for adequate safeguards, including effective oversight mechanisms. This is especially the case with NIIMS, whereby a vast amount of personal data is accessible to State, and data subjects currently have limited insight into and control over how information about them and their lives is being used.

843. Having taken judicial notice of the existence of the Data Protection Act, our focus in our analysis of the issues raised by the parties, is the extent to which the Act complies with internationally accepted standard on data protection. Parties in this respect made reference to the EU GDPR which provides for principles of data protection. This is however a regional negotiated regulation. Likewise, the United Nations Principles on Personal Data Protection and Privacy which were cited by some of the parties are only applied by the United Nations System Organizations in carrying out their mandated activities. In considering this issue, we take the view, and will be guided by the principles developed by the Organisation for Economic Co-operation and Development (OECD) namely the *OECD Privacy Principles*, which is in our view a more comprehensive and internationally recognized data privacy and protection framework that we deem most appropriate for our purposes. We also note that the said principles have been replicated in the African Union Convention on Cyber Security and Personal Data Protection.

844. The first set of principles in the *OECD Privacy Principles* relate to the collection, processing and use of data. In this respect, the Collection Limitation Principle, which provides that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. In addition, the Data Quality Principle provides that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

845. Thirdly, the Purpose Specification Principle provides that the purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. The Use Limitation Principle provides that personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject; or with the authority of law.

846. Principles 1 to 3 on processing of data in Article 13 of the African Union Convention on Cyber Security and Personal Data Protection in this respect provides for similar principles of consent and legitimacy, lawfulness and fairness, and purpose, relevance and storage.

847. The Data Protection Act has provided for detailed principles on collection, processing and transfer of data in Parts IV, V, and VI of the Act. In particular section 25 of the Act provides for and summarises the principles of personal data protection as follows:
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 165 of 205.

“25. Principles of data protection

Every data controller or data processor shall ensure that personal data is—

- (a) processed in accordance with the right to privacy of the data subject;***
- (b) processed lawfully, fairly and in a transparent manner in relation to any data subject;***
- (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;***
- (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;***
- (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;***
- (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;***
- (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and***
- (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.”***

848. The elements of these principles are detailed in subsequent sections of the Act. The next set of principles in the OECD Privacy Principles relate to the storage and rights to collected data. The Security Safeguards Principle provides that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. The Openness Principle requires general policy of openness about developments, practices and policies with respect to personal data. Furthermore, that means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

849. Under the Individual Participation Principle, and an individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

850. Lastly, under the Accountability Principle, a data controller should be accountable for complying with measures which give effect to the Privacy Principles. It is notable that the African Union Convention on Cyber Security and Personal Data Protection in this respect provides for the principles of accuracy, transparency, confidentiality and security as principles 4 to 6 in Article 13.

851. The Data Protection Act in this respect provides for an independent office of the Data Commissioner, who is appointed by the Public Service Commission, to oversee the implementation of the Act, and who is also given power to register data controllers and processors. Data Controllers are defined as the persons or entities that determine the purpose and means of processing of personal data, while data processors are the persons or entities that process data on behalf of the Data Controller. The Act also provides for the rights of Data Subjects including rights of access to personal data and correction or deletion of misleading data. It also details the procedures for rectification and erasure of personal data. Lastly, the Act has an enforcement section which among other provisions provides for a procedure for complaints and offences for unlawful disclosure of data. The Data Commissioner is required to give an Annual Report to the relevant Cabinet Secretary, and may carry out audits of data controllers.

852. While we find that the Data Protection Act has included most of the applicable data protection principles, we noted that the Registration of Persons Act is not one of the Acts to which the Data Protections Act applies as part of the consequential amendments. This notwithstanding, since one of the objectives of the Act is the regulation of the processing of personal data, whose definition as we have already found includes biometric data collected by NIIMS, it is our finding that it also applies to the data collected pursuant to the impugned amendments. We also note that there are a number of areas in the Data Protection Act that require to be operationalized by way of regulations, including circumstances when the Data Commissioner may exempt the operation of the Act, and may issue data sharing codes on the exchange of personal data between government departments. It is our view that these regulations are necessary, as they will have implications on the protection and security of personal data.

853. Once in force, data protection legislation must also be accompanied by effective implementation and enforcement. The implementation of the Data Protection Act 24 of 2019 requires an implementation framework to be in place, including the appointment of the Data Commissioner, and registration of the data controllers and processors, as well as enactment of operational regulations. Therefore, it is our finding that while there is in existence a legal framework on the collection and processing of personal data, adequate protection of the data requires the operationalization of the said legal framework.

854. The second front of the arguments put forward on the protection and security of the personal data to be collected pursuant the impugned amendments relate to the design and implementation of NIIMS. There were three limbs to these arguments. The first limb of the arguments made by the Petitioners in this regard was that extensive personal information is being collected by NIIMS in a centralized database which is linked to other functional databases, exposing it to breaches and unauthorised disclosure.

855. The 1st Petitioner submit in this respect that it is clear from the Respondents' evidence and public statements that NIIMS and the *Huduma Namba* associated with it are designed to create a cross-fertilized web of databases containing personal data of all sorts, and the Respondents have not provided any evidence to suggest that the NIIMS database and other government databases will *not* be linked in any way. In its view, the Respondents have not controverted the Petitioners' *prima facie* case that the databases will seed each other, permitting invasive searches using a single unique identifier that links across multiple government databases. Furthermore, that, contrary to the assertions of the Respondents and their experts, NIIMS fails to capture the more recent innovations developed to strengthen data protection in the Aadhaar system, let alone other options that would not establish a massive, centralized biometric database.

856. The 1st Petitioner contends that the 5th Respondent's expert witness, Loyford Muriithi, states in his affidavit that the NIIMS database will not have access to functional data, except on a "need basis," but also states that the NIIMS database "cannot access functional data" stored in institutional databases. Thus, the assertion, without any support, is internally contradictory and conflicts with multiple other descriptions of the NIIMS database by the Respondents' other experts.

857. Accordingly, that there are no legal limitations on access between the NIIMS database and functional databases, and no verifiable public information on the technical structure of the system precludes it. Furthermore, that the Respondents' evidence misstates the inevitability of a centralized master population registry model, and that the seeding of data from one database to another further undermines the argument that NIIMS could conceivably be considered data-minimal. The 1st Petitioner submits that the real hazardous data trail comes not just from the master population register, but also from all the other databases that are linked using *Huduma Nambas* and the authentication logs. It was pointed out in this regard that the absence of integration and seeding between *Aadhaar* and functional databases is a chief reason that the system was upheld in the **Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others** (*supra*).

858. The 2nd Petitioner submissions on this limb were that NIIMS will be accessible to various government agencies from the centralized data base, which re-affirms the fear that biometric data stored therein will be susceptible to meddling by third parties. The 2nd Petitioner submits that there is no evidence that encryption will guarantee the security or privacy of the said information. Moreover, there are no regulations, principles or standards against which the propriety or sufficiency of the security systems purportedly deployed for NIIMS can be measured and no attempt has been made to demonstrate, by way of actual verifiable evidence, that NIIMS does have the security features the Respondents say they have.

859. The 2nd Petitioner further argues that it has not been demonstrated that it is even necessary for other Ministries, Departments and State agencies to directly access NIIMS for purposes of 'authentication or verification of identification', as opposed to requesting for authentication from the central database and thereby eliminate the need for third party access. It was submitted that the fact that NIIMS was purportedly developed by the State and is under the exclusive control of the State engenders the idea of a monopoly of data collection, processing, storage and use contrary to best practice and standards for data protection. In conclusion, the 2nd Petitioner submits that the objects and benefits of centralized databases are

far outweighed by the potential risks to fundamental rights and freedoms attendant on the said databases.

860. The 3rd Petitioner did not specifically address this limb in their submissions, while the 5th Interested Party counsel contends that while collation of information into one database would make work easier, this does not constitute a necessary reason to violate one's privacy. Furthermore, that one of the effects of collating all the information into one database would be that of State surveillance, as acknowledged by the Supreme Court of Jamaica in the **Julian Robinson Case** (*supra*).

861. Closely related to the first limb of the Petitioners' arguments on the design of NIIMS, is the second limb that the legal and technical principles on data protection and security were not incorporated in the NIIMS system design and architecture. This aspect was mainly addressed by the 2nd Petitioner, who submitted that by their own testimonies, the Respondents have demonstrated that the NIIMS software was developed contrary to established international norms, standards and best practices for similar identity systems, including the recommendations of their own expert witness, Mr. Brian Omwenga, in his report titled **Principles Of Government Enterprise Architecture**.

862. The 2nd Petitioner further submits that some of the core principles of data protection is that personal data should be collected for specified, explicit and legitimate purposes. In addition, that the principle of data minimization requires that personal data collected be adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected. The 2nd Petitioner further argued that at the very least, the digital identification related technical standards employed for NIIMS should be well documented including standards for platform independence for interoperability, network security, incident handling, database security, and critical infrastructure security. As it were, they argued that those omissions offend the principles of transparency and accountability under Article 10 of the Constitution and essentially surrender the safety and security of vital personal information to the whims of the State.

863. Lastly, the 2nd Petitioner submits that any and all implementation tools designed by the Respondents for NIIMS, including the data capture forms, ought to be anchored in law and regulations for certainty and oversight. Therefore, that all information gathered under the impugned amendments was unlawfully gathered using a data capture form whose legal status is, by the Respondents' own admissions, unknown in law.

864. The Respondents defended the NIIMS architecture and design in their submissions. The 2nd and 3rd Respondents submit that the NIIMS database would be linked with functional databases for purposes of enabling functional institutions such as the Directorate of Criminal Investigations to request for authentication of identity of individuals. To that effect, the NIIMS database will be accessible to functional databases, whilst functional databases will be inaccessible to the NIIMS database, which is a concept of data-minimization architectural design that ensures high security and integrity, and that it retains purely identity information.

865. The 2nd and 3rd Respondents further submit that there are measures in place to ensure the safety of personal identity information collected in NIIMS as follows:

- (a) Encryption of the requisite biometric and biographical information at the point of capture by the NIIMS data capture kits (at the point of registration).

(b) Transmission of the encrypted data to the requisite servers for deduplication.

(c) The templates of biometric and biographical information stored in the NIIMS database are encrypted as well.

It was their submission that any data breach of the NIIMS database would only reveal encrypted templates of personal identity information, which cannot be unmasked without the requisite decryption key.

866. The 5th Respondent also maintain that there are sufficient safeguards in law and that Kenya has adequate infrastructure to protect data, and point to the various levels of security applied to safeguard the collected data, namely that the data is encrypted, and access is restricted using almost impenetrable and highly sophisticated mechanisms in line with international best practices, assuring confidentiality and integrity of data. Further, that NIIMS adopted UNICEF remedial measures which addressed the gaps in data sharing protocol between government agencies, underwent sufficient tests and trials, and was benchmarked on errors that was a problem in other jurisdictions including India, in order to provide a system that will not be threatened by malicious individuals.

867. The 5th Respondent further submits that their experts had demonstrated that there are no deficiencies in the NIIMS system design, and that the data in the custody of the State is well secured. That Mr. Brian Omwenga, who was its expert witness, was categorical that access and security of the data is subject to three common modes of authentication, namely, something you know, such as a password; something you have, such as an access card; and finally something you are, such as biometrics. Further, that the said expert stated that any or all of three modes of authentication may be incorporated in identity systems, and that while it has become common practice to combine the said modes, it is generally agreed that a most robust factor of authentication and identification is based on biometrics.

868. It was the further submission of the 5th Respondent that the evidence of the expert witness was that identity systems entail the maintenance of population registers which contain selected personal information, including biometrics, pertaining to each member of the resident population of a country, and that the population registers may either be centralized, decentralized or a combination of both. Further that they could also be manual or electronic, and that the United Nations Principles and Recommendations for a Vital Statistics System, provides that a population register need not take a specific form.

869. It was also argued by counsel for the 8th and 9th Interested Parties that the use of integrated databases, including DNA databases is now one of the most effective tools in fighting crime especially crimes involving violence, terrorism and sexual offences. The said Interested Parties argue that the consolidated Petitions are predicated on the theory that governments should be treated with suspicion and are not to be trusted with data or are incapable of responsibly dealing with data, yet millions of Kenyans have entrusted their most private data with private entities and social media companies including Facebook, Twitter, Tinder, and Google, who retain such data in cloud repository servers.

870. The last limb of the arguments made on the inadequacy of the safeguards of personal data, was on the paucity of information on the security features of NIIMS. The 1st Petitioner's submissions on this aspect were that the thrust of the Respondents' arguments were on "security by obscurity", which is a largely elementary and discredited approach to data

security, and is also a convenient means of ensuring that neither the Petitioners, nor this court, nor any data subject, will be able to verify the truth of the Respondents' unsupported assertions concerning the security of data, the technical constraints on purpose creep, or any of the other design features that might mitigate the concerns raised in these petitions, given that once a biometric system is compromised, it is compromised forever.

871. The 1st Petitioner further submits that the Respondents have furnished no information on how individuals will learn of, let alone address, flaws in original data registered associated with their person, or false positives and negatives generated through the (non-public) algorithms being employed, at any stage (enrolment or authentication, for example). In addition, that there is no information concerning how the Respondents will address discrepancies in existing administrative data housed in functional institutional databases.

872. The 2nd Petitioner on its part submits that Loyford Muriithi one of the Respondent's experts, in his evidence on cross-examination admitted that a certain level of information on architecture can be shared without compromising the system, to facilitate critique and understanding of the system by persons skilled in the art of information technology. Yet, that no such information has been shared with the Kenyan public despite the clear constitutional directive under Article 10. Therefore, that the inevitable conclusion in the circumstances is that the public was deliberately misled with promises of better services by NIIMS, without any information on risks attendant to centralized mass personal data in the system whose security, if any, is clouded in opaqueness and mystery.

873. The 5th Respondent responded to this argument by submitting that information on NIIMS ought not to be made available to every well-wisher as that would make it susceptible to compromise. That in the interest of national security, access to information is limited to avoid placing national data into jeopardy. Reliance was placed on the decision in **Trusted Society of Human Rights Alliance & 3 Others v Judicial Service Commission [2016] eKLR**, where the Court held that exceptions to the right to access information apply where there is a risk of substantial harm which is greater than the overall public interest in having access to the information.

874. Our analysis will address all the three limbs of argument made, as they all relate to the safety and security of the NIIMS design and its implementation framework. We received detailed testimony on the architecture and design of NIIMS, in particular as to its procurement, whether it is a centralized database or decentralized database or both, the standards that apply to the architecture of identification systems, and whether NIIMS is using closed or open source technology. We note in this regard that even though arguments were made on the procurement of NIIMS, and participation of the companies known as OT Morphi or Idemia in the process, no evidence was tabled before this Court on the process of tendering and of the award of the tender of NIIMS. We are therefore not able to make any findings on the procurement of NIIMS.

875. In addition, while the architecture and the design of a biometric identification determines how the components of the system are organized and integrated, including the ways the flows and transfers of data take place, and the specifications of where the data will be stored and how it will be accessible, it is beyond the scope of this Court's jurisdiction and capabilities to prescribe the choices that can be made in such a system's architecture and design. We are also of the view that legislation that aims to regulate technology driven innovations should not depend on the particularities of a given technology at a particular time,

as biometric technologies will further evolve, and cannot be the criterion for issuing legislative obligations. For these reasons, we are also not able to make any specific finding as invited by Mr. Anand, the 1st Petitioner's expert witness to do, on the archaic, progressive or other nature of NIIMS.

876. We will therefore restrict ourselves to the risks to the right to privacy and to data protection of data attendant with the design of, and security of NIIMS, that will require legal intervention. In this respect we are persuaded by the evidence of Dr. Fisher, the 1st Petitioner's expert witness as to the risks that may arise with biometric identity systems. He deposed that identity systems can lead to exclusion, with individuals not being able to access goods and services to which they are entitled, thus potentially impacting upon other rights, including social and economic rights. He stated that exclusion as a result of an identification system can come in two forms. Firstly, in cases where individuals who are entitled to but are not able to get an identification card or number that is used for service provision in the public and private spheres. Secondly, that even people enrolled on to biometric systems can suffer exclusion arising from biometric failure in their authentication.

877. On data breaches, Dr. Fisher averred that breaches associated with identity systems tend to be large in scale, with rectification either being impossible or incurring a significant cost. Further, that the breaches affect individuals in a number of ways, whether identity theft or fraud, financial loss or other damage. His view was that the more data and the more sensitive that data, the higher the risk. With regard to the concern of function creep, Dr. Fisher averred that the mere existence of data in a centralised identification system leads to the temptation to use it for purposes not initially intended, what he referred to as 'mission or function creep'.

878. The concerns of access to and retention of data was explained by Dr. Fisher as arising from the fact that the introduction of an identity system entails the mass collection, aggregation and retention of people's personal data which has implications on the right to privacy. It was his averment therefore, that adequate safeguards should be put in place to ensure that such data is relevant and not excessive in relation to the purposes for which it is stored, and that it is preserved in a form which permits identification of the data subjects for no longer than is required. Further, that the law must also afford adequate guarantees that retained personal data is efficiently protected from misuse and abuse.

879. Mr. Anand, similarly raised similar concerns in his evidence about the purpose free architecture of NIIMS, its lack of data minimization, its exclusionary design, and the risks of mass surveillance, breaches and fraud during decryption of data.

880. Our view as regards the centralized storage of the biometric data of data subjects is that there will be risks of attacks or unauthorized access which exist with any storage of other personal data, but the most important risks are related to the misuse of the biometric data because this is data which are uniquely linked with individuals, which cannot be changed and are universal, and the effects of any abuse of misuse of the data are irreversible. The misuse can result in discrimination, profiling, surveillance of the data subjects and identity theft. In addition, as a result of the central storage of biometric data, in most cases the data subject has no information or control over the use of his or her biometric data.

881. The report of the United Nations High Commissioner for Human Rights on *The Right to Privacy in the Digital Age* indicated as follows in this regard:

“The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person’s life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual’s rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place.”

882. We also note that these risks will also arise where the storage of biometric data is distributed between a central and federated or decentralized databases, which can be sometimes even amplified. In particular, there will be increased risks of unauthorized access and use and tracking of personal data during the process of linking the information, and the possibilities for re-use for unintended purposes of data held in decentralized databases. For these reasons, biometric data should be protected at every phase by the system design, from the collection, processing, use and retention of the data, and in all types of biometric identification databases, whether centralized or decentralized.

883. It is our conclusion therefore that all biometric systems, whether centralised or decentralised, and whether using closed or open source technology, require a strong security policy and detailed procedures on its protection and security which comply with international standards. We were referred to some of the applicable principles and standards that should govern the design and architecture of NIIMS in relation to its data, its application, technology, architecture and security, by both the Petitioners and Respondents’ experts, and which are highlighted in the report by Mr. Brian Omwenga on **Principles Of Government Enterprise Architecture**.

884. For our purposes, what is relevant is that the said principles and standards should be provided and actualized in regulations that will govern the operation of NIIMS. In addition, the biometric data and personal data in NIIMS shall only be processed if there is an appropriate legal framework in which sufficient safeguards are built in to protect fundamental rights. An example of similar Regulations in India that were framed under the Aadhaar Act, were the Aadhaar (Enrolment and Update) Regulations, 2016, The Aadhaar (Authentication) Regulations, 2016, The Aadhaar (Data Security) Regulations, 2016 and the Aadhaar (Sharing of Information) Regulations, 2016.

885. In this respect, while the Respondents explained the measures they have put in place to ensure the safety of the data collected by NIIMS and the security of the system, including the encryption of the data and restricted access, it was not disputed by the Respondents that there is no specific regulatory framework that governs the operations and security of NIIMS. The Respondents also did not provide any cogent reason for this obvious gap. To this extent we find that the legal framework on the operations of NIIMS is inadequate, and poses a risk to the security of data that will be collected in NIIMS.

886. Lastly, on the arguments made on the paucity of information on the security and safeguards of personal data provided by NIIMS, we note that the Petitioners did not bring any

evidence of having complied with the Access to Information Act, for us to find a violation on this account. The procedures for accessing information are set out in sections 8 to 11 of the Access to Information Act, which includes that an application for access to information should be made by an applicant who shall provide details and sufficient particulars for the public officer or any other official to understand what information is being requested.

887. Therefore, the duty to disclose any information on NIIMS on the part of the Respondents will only arise where there is a request made and there is a refusal by the Respondents to disclose. No such evidence of such request and refusal was presented by the Petitioners, and it is thus our finding that their arguments on this front did not have a legal basis.

Whether the Impugned Amendments are an Unnecessary, Unreasonable and Unjustifiable Limitation.

888. The 1st Petitioner submits that if the Court finds that a limitation to a right is provided by law such as the amendments to the Registration of Persons Act, then it should proceed to the proportionality analysis contained in Article 24(1). It cites the cases of **Kenya National Commission on Human Rights & Another vs Attorney General & 3 Others, [2017] eKLR** and **Jacqueline Okuta & Anor vs Hon. Attorney General & 2 Others, Petition No. 397 of 2016**, for the position that the determination of the issue whether a law that limits rights is justified is by arrived at by asking whether the law is proportionate. Further, that proportionality is defined as ‘the set of rules determining the necessary and sufficient conditions for a limitation on a constitutionally protected right by a law to be constitutionally protected’, the elements of which are delineated in Article 24(1).

889. The 1st Petitioner cites the Jamaican Supreme Court decision in the **Julian J Robinson Case** which opted for “the strict application” of the proportionality test as “the best way to preserve fundamental rights and freedoms”. Further, that in **Geoffrey Andare v Attorney General & 2 others [2016] eKLR** the court extensively relied on the Oakes Test in interpreting the Constitution in a manner that advances the rule of law and human rights.

890. The 2nd Petitioner on its part cites the case of **Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR** for the test against which limitation of any right recognized under the Bill of Rights may be permitted under Article 24 of the Constitution. It submits that under Article 24(3) of our Constitution, the burden of proving the reasonableness and proportionality of any limitation of a fundamental right is expressly reposed in the state and has to be discharged on a high standard based on cogent and persuasive evidence. The case of **Robert Alai v The Hon Attorney General & Another [2017] e KLR** was cited in this regard.

891. According to the 2nd Petitioner, when held against the above standards, it is clear that the Respondents have merely strived to justify the purpose of NIIMS amendments without cogent and/or persuasive evidence to demonstrate that the stated purpose is sufficiently important to warrant overriding the fundamental right to privacy and connected rights; or that the measures adopted have been carefully designed to achieve the stated purpose of NIIMS; or that the means used to achieve the stated objectives of NIIMS are the only available and viable alternatives that would least violate the right to privacy; or that the benefit arising from the violation is in fact greater than the harm to the right.

892. The 3rd Petitioner on its part points out that Article 24 of the Constitution sets out clear, concrete and objective circumstances in which a right or fundamental freedom in the Bill of Rights may be limited.

893. The 5th Interested Party introduces the argument that the collection of personal information as was done to implement NIIMS was *ultra vires* the Registration of Persons Act, since the information collected using the data capture form is identical to the information to be collected by the Principal Registrar under Section 5 of the Registration of Persons Act. According to the 5th Interested Party, the power to collect that kind of information is only reserved for the Principal Registrar. For this reason, counsel urged the court to find that the Registration of Persons Act does not grant any powers to any person to collect personal information under NIIMS, and the information collected during the mass registration exercise was therefore unlawful and consequently unconstitutional. It is however noted by this Court that the Petitioners did not plead this specific illegality in their Petitions, and the Respondents therefore had no opportunity to respond to matters being raised by the 5th Interested Party for the first time in submissions.

894. The 6th Interested Party submits that the Respondents deliberately sought to circumvent Article 24 of the Constitution by pretending that the amendments are minor and of no significance. However, that as long as it is demonstrable that the amendments threaten and/or limit a fundamental right or freedom, the Respondents cannot escape the requirement to comply with Article 24 of the Constitution. According to the 6th Interested Party, the amendment to the Registration of Persons Act to include biometric data is excessive, unwarranted, unreasonable and unjustifiable in an open and democratic society and impacts directly on an individual's right to privacy and bodily integrity secured under Article 31 of the Constitution.

895. Further, that the requirement or collection of DNA of any individual is generally and widely recognised to be the exception rather than the norm and its retrieval or collection must be for a specific proven purpose, specifically authorised by a legal warrant where proved to be necessary and on a case-by-case basis. In addition, that the data is easily susceptible to serious abuse and/or misuse in the wrong hands that can lead to irreparable damage including security threats to individuals.

896. The 1st Respondent submitted on this issue in rebuttal, and contends that the Constitution sanctions the requisition or revelation of one's private affairs or that of the family where necessary. It beseeched the court not to adopt the Jamaican decision in **Julian J Robinson Case** (*supra*) on the basis that the Court has the obligation to place those decisions in their rightful context whenever it applies comparative jurisdiction. They urged the Court to find persuasion in the dissenting opinion in **In the Matter of the Principle of Gender Representation in the National Assembly and the Senate** [2012] eKLR .

897. It was the 1st Respondent's submission that there was a clearly set out legitimate State aim in seeking the information; to create an integrated national identity management system. To further emphasize the fact that constitutional rights are not absolute, the 1st Respondent finds persuasion in **R vs Director of Serious Fraud Office, ex parte Smith** [1993] AC 1, where it was held that *few* would dispute that some curtailment of the liberty is indispensable to the stability of society.

898. In conclusion, the 1st Respondent submits that the amendments in issue were legal, contemplated in the Constitution and for a defined legitimate State aim. That it accounts for Petition 56, 58 & 59 of 2019 (Consolidated) | Page 175 of 205.

proportionate interference within the context of contemporary practices, developments and sophistication of life. Further, that it was in the province of the political arm of the government to determine what constitutes necessary information for government purposes, and as such Courts ought to exercise some measure of deference to the repository of the constitutional powers on matters of policy under the doctrine of separation of powers.

899. The 4th and 7th Respondents similarly submit that the right to privacy is not absolute. Therefore, that in determining the type of information that may be revealed, it would be prudent to establish the purpose/objective of doing so and the value of that information. Further, that the collection of personal information by the State is in accordance with the social contract theory, in that, when ceding their sovereignty to the State, the citizens cede control of certain aspects of their lives and give up the condition of unregulated freedom, including their personal information, in exchange for the security of a civil society governed by a democratically elected government. Reliance was placed on the decision by the European Court of Justice in Michael Schwarz v Stadt Bochum C"291/12, EU:C:2013:670 (17 October 2013) for this position.

900. The 5th Respondent echoes the arguments by the other respondents and submits that the Petitioners failed to state with the required degree of precision the manner in which the alleged threat to the right to privacy has or would be infringed. Further, that they have not demonstrated the way the Respondents intend to obtain any information for unlawful purpose. As such, the petition is hypothetical and speculative. According to the 5th Respondent, it was not disputed that the state bears the right to limit rights bargained by society upon appropriate legal criteria that meets a public interest and purpose.

901. The 5th Respondents argues that that two main standards apply when legislation limits a fundamental right in the Bill of Rights, namely, the rationality test and the reasonableness or proportionality test, in line with the provisions of Article 24 (1) of the Constitution, which provide that such a limitation is valid only if it is "reasonable and justifiable in an open and democratic society".

902. In justifying rationality of the impugned data, it was the 5th Respondent's argument that data was collected for a reasonable State objective. The 5th Respondent invited this Court to note that the right to privacy is not a non-derogable right under Article 25 of the Constitution, and cited the decision in Canadian Supreme Court in case of R vs Oakes 1 SCR 103, which restated the key principles that apply to determine whether a limitation of a right is reasonable and demonstrably justified in a free and democratic society.

903. The 6th Respondent on its part submits that the right to privacy is not absolute, and is subject to limitation as provided for in Article 24 of the Constitution. With particular respect to the impugned amendments, it was the 6th Respondent's submission that the amendments are intended to enhance development and State security and as such are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. Reliance was placed on the decision of the Constitutional Court of South Africa in Samuel Manamela & Another vs The Director General of Justice, CCT 25/99 on the interpretation of Article 24(1).

904. While justifying the fact that it did not downplay Article 24 when enacting the impugned legislation, the 6th Respondent referred to the case of Attorney General & another v Randu Nzai Ruwa & 2 others [2016] eKLR, where it was observed that interests of national security can be invoked to limit rights, if *they* are reasonable and justifiable. Further Petition 56, 58 & 59 of 2019 (Consolidated) | Page 176 of 205.

reliance on justification for the limitation of the right to privacy was placed on the decision of the Supreme Court of India in **Justice K.S. Puttaswamy (Retd.) and others vs Union of India and Others (supra)**.

905. The Respondents' positions were supported by the 1st Interested Party, who submits that all the rights which the Petitioners allege to have been infringed by the implementation of NIIMS are not absolute, and can be limited under Article 25 of the Constitution. Further, that in considering the limitation under Article 24 (1) of the Constitution, the Court must bear in mind that there are no superior rights and take into consideration, factors such as the nature and extent of the limitation and the need to ensure that enjoyment of rights and fundamental freedoms by one individual does not prejudice the rights of others. Therefore, that this calls for balancing of rights under the principle of proportionality as was held in the case of **University Academic Staff Union (UASU) vs Attorney General & others, [2018] eKLR**.

906. The 1st Interested Party also cites the case of **Robert Alai vs The Hon Attorney General & Another, [2017] eKLR** where the court observed *that* constitutionally guaranteed rights should not be limited except where the limitation is reasonable and justifiable, and the objective of that limitation is intended to serve the society. It also cites the case of **R.v.Oakes, [1986] 1 S.C.R. 103**, where the court stated that the onus of proving that a limitation on any Charter right is reasonable and demonstrably justified in a free and democratic society rests upon the party seeking to uphold the limitation.

907. It is the 1st Interested Party's view that the implementation of NIIMS is reasonable and justifiable, and meets the constitutional muster under Article 24 of the Constitution, considering that NIIMS shall ease tracing of families of separated children with special needs and by this the government shall be able to reunite these children with their families. Further, that NIIMS would curb cases of illicit adoption practices, child trafficking and permanent separation of children from their biological families. In addition, that NIIMS will facilitate the matching of resources to children socio economic needs and enable the government deliver its key constitutional mandate as envisaged in Article 53 of the Constitution of Kenya.

908. The 8th and 9th Interested Parties submissions focused on justification presented by the terrorists incidents in Kenya, and they contend that Article 24(1) of the Constitution permits limitation of the rights and fundamental freedoms in the Bill of Rights that are reasonable and justifiable, and that the greater public interest and security concerns far outweigh individual rights. They further argue that terrorist attacks have led to the curtailment of privacy through activities that are now routine, including registering identification data at nearly every public building including places of worship, and undergoing searches at all public gatherings.

909. Accordingly, they argue that the aggregation and verification of data already available to State agencies through a system such as *Huduma Namba* can thwart future attacks and deter terrorists and criminals from operating freely in the country. The 8th and 9th Interested Parties point out that the limitations to the rights in Article 31 were tested in **Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others, [2015] eKLR** where the Court found the limitations imposed on the right to privacy by the National Intelligence Service Act to be reasonable and justifiable on account of the circumstances of our nation, the adequacy of safeguards built into the law and the availability of remedies for any breach.

910. We note that the issue of whether the impugned amendments violate and limit the constitutional right to privacy has already been dealt with extensively in this judgment, and Petition 56, 58 & 59 of 2019 (Consolidated) | Page 177 of 205.

this Court has made two findings in this respect. Firstly, that other than the collection of DNA and GPS coordinates, the other biometric data that is required to be collected by the amendments is necessary for purposes of identification, and there is thus no violation of the right to informational privacy under section 31(c) of the Constitution.

911. Secondly, this Court has found that although a legal framework for protection of personal data now exists in Kenya, there are inadequacies in the said legal framework in terms of operationalization, and also in terms of the implementation and operationalization of NIIMS, to guarantee the security of the data that will be collected in NIIMS. To this extent, there is a risk that the data collected in NIIMS may be accessed by unauthorized persons or used for improper or illegal purposes, which is a threat to the right to privacy which may occur in the implementation of NIIMS. To this extent, there is the possibility of a limitation on the right to privacy

912. We commence our analysis by noting that the right to privacy is not one of the rights that cannot be limited under Article 25(c) of the Constitution. Therefore, a limitation is permissible so long as it meets the criteria set out in Article 24 (1), which provides that a right or fundamental freedom in the Bill of Rights shall not be limited except by law, and only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account the nature of the right or fundamental freedom. It was in this regard held as follows in **Robert Alai v The Hon Attorney General & another (supra)** as regards the application of Article 24(1):

“50. The principle enunciated above is that constitutionally guaranteed rights should not be limited except where the limitation is reasonable, justifiable and the objective of that limitation is intended to serve the society. The standard required to justify limitation, is high enough to discourage any limitation that does not meet a constitutional test. And that limitation to a right is an exception rather than a rule.

913. In the Canadian case of **R v. Oakes (supra)**, the Court considered the question whether section 8 of the Narcotic Control Act, which had been found to be unconstitutional for violating section 11 of the Canadian Charter of Rights and Freedom, was a reasonable limit prescribed by law and demonstrably justified in a free and democratic society. In reaching the conclusion that it was not, the Court enunciated the criteria to be followed in answering the question as follows:

“69. To establish that a limit is reasonable and demonstrably justified in a free and democratic society, two central criteria must be satisfied. First, the objective, which the measures responsible for a limit on a Charter right or freedom are designed to serve, must be "of sufficient importance to warrant overriding a constitutionally protected right or freedom": R. v. Big M Drug Mart Ltd., supra, at p. 352. The standard must be high in order to ensure that objectives which are trivial or discordant with the principles integral to a free and democratic society do not gain s. 1 protection. It is necessary, at a minimum, that an objective relate to concerns which are pressing and substantial in a free and democratic society before it can be characterized as sufficiently important.

70. Second, once a sufficiently significant objective is recognized, then the party invoking s. 1 must show that the means chosen are reasonable and

demonstrably justified. This involves 'a form of proportionality test': R. v. Big M Drug Mart Ltd., supra, at p. 352. Although the nature of the proportionality test will vary depending on the circumstances, in each case courts will be required to balance the interests of society with those of individuals and groups. There are, in my view, three important components of a proportionality test. First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair or based on irrational considerations. In short, they must be rationally connected to the objective. Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question: R. v. Big M Drug Mart Ltd., supra, at p. 352. Third, there must be a proportionality between the effects of the measures which are responsible for limiting the Charter right or freedom, and the objective which has been identified as of "sufficient importance".

914. Further, in Geoffrey Andare vs Attorney General, (supra) the Court held as follows in this regard:

"90. The questions that beg, bearing in mind the express provisions of Article 24 and the criteria in R vs Oakes are: what is the purpose of the limitation, and how important is it" What is the relationship between the limitation and its purpose" Are there less restrictive means to achieve the purpose intended"

915. Therefore, in the context of this Petition, the stated purpose of the impugned amendments of identification of persons should be based upon the rule of law, the means used to reach this purpose should not only be relevant and necessary, but also not lead to disproportionate harm and burdens for the citizens. As was held in the Julian J Robinson Case (supra), the proportionality test used to determine whether a law can be justified in a free and democratic society is a two-stage test. The first stage is that the law must be passed for a proper purpose. The second stage has three components, namely:

- a) the measure must be carefully designed to achieve the objective,
- b) the means used must violate the right as little as possible; and
- c) there must be proportionality between the measure and the effect, that is to say, the benefit must be greater than the harm to the right.

916. The propriety and sufficiency of the impugned amendments for the collection of personal data has been challenged with respect to two types of data, namely DNA and GPS coordinates. As noted by Dr. Malombe in his evidence, DNA information can have far reaching consequences as it not only reveals the identity of a given person, but also genetic properties, which include the likeliness to develop particular diseases, parentage and also family links. In addition, it can be recovered from a multitude of sources, and it provides or is likely to provide scientific, medical and personal information pertinent for a person throughout his or her life.

917. It is thus our finding, that because of the specificity of the information that DNA may disclose, and the harm this disclosure may cause not just to the data subject but other family members in terms of both identification and genetic information, DNA information requires

Petition 56, 58 & 59 of 2019 (Consolidated) | Page 179 of 205.

and justifies a particular and specific legal protection. This was confirmed by the Article 29 Working Party in its **Report on the Processing of Genetic Data**.

918. Likewise, specific authorization anchored in law is required for the use of GPS coordinates, in light of the privacy risks we have already identified in terms of their possible use to track and identify a person's location. There is also the added risk that centralized databases can use GPS information, to create "watchlists" or "blacklists" to create information on individuals to be watched and tracked. These individuals as a result become suspects, leading to a reversal of the presumption of innocence.

919. Accordingly, we find that the provision for collection of DNA and GPS coordinates in the impugned amendments, without specific legislation detailing out the appropriate safeguards and procedures in the collection, and the manner and extent that the right to privacy will be limited in this regard, is not justifiable. The Respondents in this respect conceded that they will not collect DNA and GPS coordinates, and that in any event they have no capacity to do so. However, our position is that as long as the collection of DNA and GPS coordinates remain a provision in the impugned amendments, there is the possibility that they can be abused and misused, and thereby risk violating the rights to privacy without justification.

920. This Court has also discussed at length the necessity of the biometric data that is required by the impugned amendments and the necessity of NIIMS as an identification and verification system. We have also noted that such system that stores biometric data is susceptible to risks and any breaches can cause irreparable harm to the data subjects. An inadequate legislative framework for the protection and security of the data is therefore clearly a limitation to the right to privacy, in light of the risks it invites for unauthorized access and other data breaches.

921. In addition, a law that affects a fundamental right or freedom should be clear and unambiguous. This principle was stated in the case of **Andrew Mujuni Mwenda vs Attorney General (supra)**, and was echoed in the case of **Geoffrey Andare vs Attorney General (supra)** where the court stated:-

"...The principle of law with regard to legislation limiting fundamental rights is that the law must be clear and precise enough to enable individuals to conform their conduct to its dictate..."

922. This position equally applies to any law that seeks to protect or secure personal data, particularly in light of the grave effects of breach of the data already alluded to. To this extent the lack of a comprehensive legislative framework when collecting personal data under the impugned amendments, is contrary to the principles of democratic governance and the rule of law, and thereby unjustifiable. It is also notable in this respect that no justification or reasons were given by the Respondents for this lapse, leading to our earlier conclusion that the process of NIIMS appeared to have been rushed.

Whether there was a Violation of the Right to Equality and Non-Discrimination

923. The 1st Petitioner challenges the impugned amendments on the procedural grounds relied on by the other Petitioners and supported by the Interested Parties who support the Petitions. At the core of its case, however, is the contention that the impugned amendments violate or threaten to violate the rights of members of the Nubian community and other vulnerable groups to equality and non-discrimination. The 1st Petitioner argues that the Petition 56, 58 & 59 of 2019 (Consolidated) | Page 180 of 205.

impugned amendments disclose violations of the rights to privacy, right to be free from any form of discrimination, citizenship rights, the right to dignity, as well as the right to information. It is also the 1st Petitioner's contention that the impugned amendments implicate social- economic rights as well as the rights and the best interests of the child.

924. The 1st Petitioner's arguments are set out in the submissions dated 19th June 2019 and Supplementary Submissions dated 8th October 2019. They were highlighted by the 1st Petitioner's counsel, Mr. Waikwa and Mr. Bashir.

925. The 1st Petitioner's case is premised on the contention that the system introduced by NIIMS will perpetuate the discrimination that members of the Nubian community have been subjected to over the years. It is submitted on their behalf that despite having been settled in Kenya more than 100 years ago and qualifying as citizens under Kenyan law, most of them have not been recognized as citizens and are treated as aliens, which they term as contrary to the constitutional prohibitions of discrimination. In support of this argument, it is submitted that Nubians are required to go through a long and complex vetting procedure to obtain identity cards and birth certificates necessary for recognition of their citizenship, and essential for everyday life. As a result, most of them have been unable to access the basic services offered by the State or to enjoy their constitutional rights.

926. In elaborating on the question of violation of the right to equality and non-discrimination the 1st Petitioner submits that through the NIIMS systems, the State is content to continue with the exclusionary practices under the present legal regime and leave thousands of people behind instead of fixing the present discriminatory practices. It is its contention that Nubians and other vulnerable minority groups in Kenya undergo mandatory heightened scrutiny on the basis of race, religion and tribe prior to registering as citizens and obtaining a national ID card. The averments of Ms. Fatuma Abdulrahman and Ahmed Khalil Kafe, as well as the supporting affidavit of Mr. Shafi Ali Hussein are cited in support.

927. The 1st Petitioner observes that the State has continued with the discriminatory practices despite international opprobrium and judicial censure of such practices. It contends that the Respondents have not controverted its contentions that, unlike other Kenyans, Nubians are subjected to an unfair and arbitrary vetting process in which they are required to prove their citizenship by producing extra documents such as their grandparents' birth certificates which most of them cannot reasonably access.

928. In linking up the contention of past discrimination with the system mooted under the impugned amendments, the 1st Petitioner contends that enrolment in NIIMS presents a number of potential harms that will be suffered disproportionately by Nubians and other similarly situated groups. The basis of this contention is that there are hardships which they are already being subjected to which the Respondents were aware of at the time the impugned amendments were made.

929. According to the 1st Petitioner, these hardships are, first, that individuals who have been unsuccessful in obtaining documentation of their Kenyan nationality on account of the government's discriminatory practices have been unable to enroll because enrolment hinges on possession of identity documents. The second is that the enrolment process requires an administrative determination of citizenship or non-citizenship. Accordingly, because of the ongoing effects of vetting and the exclusionary attitudes towards minorities it represents, Nubians are at a heightened risk of being "successfully" enrolled as non-citizens, even though they are entitled to Kenyan citizenship by birth. The 1st Petitioner argues that this 'quasi-Petition 56, 58 & 59 of 2019 (Consolidated) | Page 181 of 205.

denationalization' re-labeling of Kenyans as foreigners across all government systems linked to NIIMS represents a massive threat to Nubians on account of their ethnicity, race or tribe, without any safeguards put in place to prevent it, and no hint of an effective remedy.

930. The 1st Petitioner contends, thirdly, that after “successful” enrolment in NIIMS, Nubians and other communities who are heavily scrutinized and policed face a heightened risk of profiling and tracking within the system just as they do in respect of the existing national registration system. They term these failings with respect to the impugned amendments in general and NIIMS in particular as contrary to Article 27 of the Constitution.

931. The 2nd Petitioner supports the contentions by the 1st Petitioner that the impugned amendments and the NIIMS process will result in a violation of the right to equality and non-discrimination guaranteed under Article 27. It further agrees with the 1st Petitioner that the process will lead to discrimination against those communities and groups such as the 1st Petitioner, stateless persons, refugees and persons who have perennially been denied the opportunity to register for purposes of identification. It further contends that the impugned amendments have not addressed the underlying legal and institutional issues that face stateless and other undocumented persons, and that the amendments will therefore merely entrench and exacerbate these issues in the digital sphere. It is also the 2nd Petitioner’s contention that the fact that the impugned law does not expressly apply to stateless persons, refugees and aliens will lead to their continued marginalization.

932. The main contention by the 2nd Petitioner, however, with respect to violation of the constitutional right to equality and non-discrimination is that the impugned law effectively makes it mandatory to register under NIIMS and to obtain the unique identification number. It submits that under section 9A(2)(d), NIIMS shall, among other things, support the printing and distribution for collection of all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licences, work permits, passport and foreign travel documentation, and student identification cards issued under the Births and Deaths Registration Act, Basic Education Act, Registration of Persons Act, the Refugee Act, the Traffic Act and the Kenya Citizenship and Immigration Act, and all other forms of government issued identification documentation as may be specified in a Gazette Notice by the Cabinet Secretary. The 2nd Petitioner submits that from this provision, public services connected to these identification documents will only be offered to those who surrender their personal biometric information and are issued with the unique identification number known as the *Huduma Namba*.

933. It is the 2nd Petitioner’s contention that the overall effect of the impugned amendments will be to offend Article 27 of the Constitution which guarantees the right of equality before the law and explicitly prohibits discrimination on any ground. It submits that denying any person constitutionally guaranteed rights to public services based only on lack of biometric identification is unreasonable and unjustifiable in a free and democratic society.

934. The 2nd Petitioner argues that no cogent or persuasive evidence has been provided to demonstrate that the said services can only be efficiently provided using biometric data of the nature sought under the Act. To buttress its argument, it cites the decision in **R vs Big M. Drug Mart Ltd** [1985] 1 S.C.R. 295 in which the court stated that freedom means that, subject to such limitations as are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others, no one is to be forced to act in a way contrary to his beliefs or his conscience.

935. It is also its contention that the impugned amendments have not addressed the underlying legal and institutional issues that face stateless and other undocumented persons and will therefore merely entrench and exacerbate them in the digital sphere.

936. The 3rd Petitioner did not address itself to this issue, while the 3rd and 4th Interested Parties, though they indicated their support for the Petitions, did not file any submissions. The 6th Interested Party also supported the Petitions and filed submissions, but it did not address itself to the issue of alleged violation of the right to equality and non-discrimination.

937. In its submissions in support of the Consolidated Petitions, the 5th Interested Party agrees with the 1st and 2nd Petitioners that the impugned amendments would lead to violation of Article 27, for various reasons. It argues that the collection of biometric identifiers during the registration process implies an intent by the State to subsequently use biometric identifiers for authentication of identity. In its view, this Act, coupled with the messaging from the State that *Huduma Namba* will be needed in order to access government services as set out in the Data Capture Form, implies several things which the 5th Interested Party deems detrimental to fundamental rights. It submits, first, that the mass registration exercise is not the only time biometric identifiers will be collected by the State; that biometrics will be required at the point of service to determine the authenticity of the person being served; and that this may happen every time a person requires services from any government agency.

938. Its second contention is that all government agencies will have a copy of the biometric identifiers which they will use to authenticate identity of every person served, and every agency with access to this information can tell the behavioural patterns of a data subject from the digital footprint left at every authentication. It is its submission that this creates a fertile basis for covert surveillance, and even if such information was only to be held by one agency, there would still be potential for surveillance, which is frowned upon under the Constitution. It cites in this regard the decision in **Kenya Human Rights Commission v Communication Authority of Kenya & 4 others** [2018] eKLR. In the 5th Interested Party's view, such surveillance could lead to profiling, which in turn could lead to discrimination, and the effect of such a system is therefore unconstitutional.

939. The contention that the impugned amendments will result in violation of Article 27 is strenuously contested by the Respondents. The 1st Respondent submits, first, that the 2nd Petitioner had, in its written submissions, admitted that the text of the amendments in issue in and of itself was not discriminatory. In the 1st Respondent's view, to the extent that the Petition is premised entirely on the constitutionality or otherwise of the enactments in issue, the admission was dispositive of the issue. This was because what was at issue was not the administrative practices of the Respondents but constitutionality or otherwise of the amendments. We observe at the outset that our perusal of the submissions by the 2nd Petitioner have not disclosed this alleged admission on its part.

940. It is also the 1st Respondent's contention that there is no material placed in evidence before the court, save for the bare and general allegation of discrimination by the 1st Petitioner, to support its allegation of discrimination. Such material, in the 1st Respondent's view, would have consisted of cogent evidence from specific members of the Nubian community on the alleged discrimination. In the absence of such evidence, the claim of discrimination remained unproven. To the 1st Respondent, the pilot projects on NIIMS, which were conducted in several locations within the Republic including Kibera and Eastleigh North in Nairobi County, as well as those undertaken in Marsabit and Wajir counties where no

issues of discrimination arose, are pointers that there is no discrimination in the implementation of NIIMS.

941. With regard to the reliance by the 1st Petitioner on the African Commission of Human and People's Rights decision as a basis for the claim that there was discrimination against members of the Nubian community, the position of the 1st Respondent is that the said Commission is not a judicial body and its recommendations are neither conclusive nor binding. Further, that in any event, the said Commission has in reported cases before the African Court on Human and Peoples' Rights submitted that it does not have confidence in Kenya's judicial processes in giving timely and effective redress. It is his contention further that the Commission, which is actively engaged in legal proceedings against the Republic of Kenya, cannot be said to be impartial towards the Republic of Kenya. The 1st Respondent further takes the position that the report by the African Commission has no nexus in any way with the legislative amendments in issue.

942. The 1st Respondent takes the position that the 1st Petitioner has no justiciable controversy in its Petition before this court. It relies on the decision in **Patrick Ouma Onyango & 12 Others v the Attorney General & 2 Others**, Misc Appl No. 677 of 2005 in which the court took the view that "[i]n order for a claim to be justiciable... it must 'present a real and substantial controversy which unequivocally calls for adjudication of the rights asserted.'" It is its submission that in the present case, the entire ground alleging discrimination is premised on mere apprehension not directly attributable to the enactments in issue. Rather, it has its basis on alleged past administrative action that has never been subject to judicial inquiry and determination.

943. In their submissions, the 2nd and 3rd Respondents also oppose the allegation that the impugned amendments and the NIIMS process will result in discrimination against the 1st Petitioner and other marginalised communities. They note that the 1st Petitioner challenges the impugned amendments on the basis that sections 3, 5 and 9 of the Act would perpetuate discrimination against members of the Nubian Community who are allegedly being discriminated against under the current registration systems. The 2nd and 3rd Respondents deny that this is the case. They rely on the definition of discrimination in the case of **Jacqueline Okeyo Manani & 5 Others v. Attorney General & Another** [2018] eKLR.

944. The 2nd and 3rd Respondents note that from the above decision, the elements of discrimination are unequal treatment, unfavourable bias and bias based on the constitutional definition of discrimination.

945. They submit that contrary to the allegations by the 1st Petitioner, NIIMS does not meet the above elements. This is because, first, the Act as amended does not make any distinction in the registration of persons onto NIIMS, and the Act is clear that all residents are free to enlist onto NIIMS. They further submit that the Kenya Citizenship and Immigration Act, 2012 already provides for the criteria and process of registration of foreigners in Kenya, including the stateless, as does the Refugees Act, 2006, with respect to refugees residing in the country. Their submission is that NIIMS does not replace these existing processes, systems and documents.

946. According to the 2nd and 3rd Respondents, the 1st Petitioner's contentions are based on a misapprehension of the role to be played by NIIMS. Their case is that the Act does not confer citizenship. On the contrary, it is based on pre-existing laws on citizenship and registration which are all perfectly constitutional. They illustrate their position by citing the Kenya Petition 56, 58 & 59 of 2019 (Consolidated) | Page 184 of 205.

Citizenship and Immigration Act, 2012, the Refugees Act, 2006, and the Children Act to submit that since these Acts are presumed to be constitutional, and since NIIMS is based on them, it cannot therefore be deemed to be discriminatory or unconstitutional.

947. The 2nd and 3rd Respondents maintain that the documents under the respective Acts would continue to be issued under the existing framework, which means that passports would be issued under the provisions of the Kenya Citizenship and Immigration Act; births and deaths certificates under the Births and Deaths Registration Act; while refugee and alien cards would be issued on the basis of the Refugee Act and the Kenya Citizenship and Immigration Act respectively. Their submission is that none of these documents would be issued under the Statute Law (Miscellaneous Amendments) Act No 18 of 2018. Further, that NIIMS does not introduce any new requirements outside of the existing legal framework, nor does it contain any provision that fosters discrimination.

948. With regard to the 1st Petitioner's contention that NIIMS would perpetuate discrimination against members of the Nubian community due to the requirement for vetting, the 2nd and 3rd Respondents submit that this allegation has no basis. This is because it is not sections 3, 5 and 9 of the Act that introduced vetting as a process for the issuance of identification documents to the Nubians or any other border community. They ask the court to take judicial notice of the fact that vetting committees are a legally sanctioned part of the process of issuing identification documents pursuant to section 23 of the Security Laws (Miscellaneous Amendments) Act, 2014 which amended the Act by adding section 8(1A) on vetting.

949. They contend that despite the fact that vetting only applies to border communities, this does not make it discriminatory within the meaning of Article 27 of the Constitution. They rely in support of this submission on the decision in **John Harun Mwau v. Independent Electoral and Boundaries Commission & Another** [2013] eKLR.

950. The 2nd and 3rd Respondents emphasise, on the basis of the averments by Dr. (Eng.) Karanja Kibicho in his affidavit of 14th May 2019, that the process of vetting is neither a creature of the impugned amendments nor is it targeted at the Nubians only. It is also their submission that vetting is necessitated by, among other factors, national security and the fact that all individuals must prove their nationality before being issued with national identification documents. It is their submission that in any event, the question of the vetting process for border communities falls outside the purview of section 9 of the impugned amendments and of this matter. They reiterate that the impugned amendments are not in any way discriminatory against the 1st Petitioner or any other individuals residing in the country.

951. With regard to the reliance by the 1st Petitioner on the decisions of the African Commission and the African Committee on the Rights and Welfare of the Child, it is their submission that while the African Commission is mandated under the ACHPR to hear communications on violation of rights under the Charter and make recommendations, its recommendations are not legally binding on States, nor does the Charter obligate States to implement the recommendations of the Commission. They submit, however, that States are at liberty to implement such recommendations based on the principle of good faith based on their ratification of the African Charter. The 2nd and 3rd Respondents cite in support Nelson Enonchong's article "**The African Charter on Human and Peoples' Rights: Effective Remedies in Domestic Law**" in which he notes that:

“the African Commission has no jurisdiction to make binding decisions against state parties that have violated the provisions of the Charter. Once the Commission reaches a decision on the merits of a case, its only jurisdiction is to make recommendations to the Assembly of Heads of State and Government (AHSO) of the African Union (previously Organization of African Unity). But the AHSO itself cannot make binding decisions against state parties. It can only decide to permit publication of their violations.”

952. It is their submission that the above position notwithstanding, the Government of Kenya has implemented measures aimed at ensuring that Nubians and all other perceived marginalized communities are registered as citizens. They assert that it is within the knowledge of the 1st Petitioner that the government acknowledged and endeavored to ensure equality and non-discrimination against the Nubian Community. They draw the court’s attention to the letter dated 8th April, 2017 in which the 1st Petitioner acknowledged that the Government, through the National Registration Bureau, had taken commendable measures for the registration of Nubians.

953. The 2nd and 3rd Respondents assert that in any event, the recommendations of the African Commission and the African Committee on the Rights and Welfare of the Child cannot be implemented through constitutional petitions such as the instant ones, as the said recommendations were not based on interpretation of the Constitution of Kenya.

954. The 4th and 7th Respondents note that the challenge to NIIMS on the basis that it will perpetuate discrimination is based on the vetting procedures in obtaining an identification card as a prerequisite for registration in NIIMS, as emerged from the testimony of Ahmed Khalil Kafe (PW 3), Mr. Ali Shafi Hussein (PW 4) and Ms. Fatuma Abdulrahman (PW 5). They note that these witnesses all said that they had no issue with the *Huduma Namba*, their problem being with the vetting procedures that members of the Nubian community undergo in obtaining identification cards.

955. The 4th and 7th Respondents submit that, as outlined by Dr. Karanja Kibicho (RW 3), every person who applies for an identification card undergoes a form of vetting in which the Assistant Chief of the applicant’s locality must be able to first identify the applicant prior to approving the application. It is their submission that the 4th Respondent is clothed with the discretion, pursuant to section 8 of the Act, to require further information from an applicant on a case by case basis. They submit that the constitutionality of section 8 of the Act is not challenged in the present proceedings, and the procedure set out in the section enjoys the presumption of constitutionality.

956. The 4th and 7th Respondents further note that the 1st Petitioner’s witnesses, Mr. Hussein and Ms. Abdirahman, stated in their evidence that they are aware of two levels of vetting for the Nubian community, the first stage of which is by members of the Nubian community. It is their submission that no government official is involved in this stage of the vetting, and it is only the members of the Nubian community themselves who have the initial mandate to confirm the authenticity of the applicant’s claim to Kenyan citizenship. The second level of vetting, according to the 4th and 7th Respondents, is the one that involves committees comprising government officers. They note that while the 1st Petitioner has raised concerns about the representation of the Nubian community in this second level, Dr. Kibicho had clarified that the decisions of the committee are not based on majority voting.

957. It is their submission that, in any event, the concerns raised by the members of the 1st Petitioner are in respect to a process which is separate from NIIMS. They contend that the 1st Petitioner has not challenged the NIIMS process in these proceedings, nor does its witnesses, in their evidence, demonstrate the manner in which the vetting process is arbitrary, unreasonable or without a basis.

958. It is also the submission of the 4th and 7th Respondents that as testified by Dr. Kibicho, NIIMS is a continuous process. Accordingly, members of the Nubian community as well as any other person who is yet to acquire an identification card or a birth certificate will be able to register through NIIMS once they acquire these documents.

959. While observing that Shafi Hussein had, in his testimony, maintained that having had a three-step perspective of NIIMS registration, that is prior to, during and after the mass registration exercise, his concerns on the alleged discrimination remain, the 4th and 7th Respondents submit that his testimony could not be given credence given that he admitted that he had not registered for a *Huduma Namba* and could not therefore comment on the process. They further observe that he had admitted that he did not undergo vetting when applying for an identification card.

960. The 4th and 7th Respondents submit that the 1st Petitioner had failed to demonstrate how members of the Nubian community had been denied equal protection or benefit of the law. They note that Dr. Kibicho had testified that various initiatives have been put in place to facilitate the issuance of identity cards to Nubians, such as the Rapid Response Initiative (RRI), a fact which Shafi Hussein (PW 4) had acknowledged in his letter to the 4th Respondent dated 8th April 2017.

961. The 4th and 7th Respondents also agree with the rest of the Respondents that NIIMS will not result in discrimination against the 1st Petitioner's members or any other group. They submit that the contention that the deployment of NIIMS was discriminatory to the Nubian community because they undergo vetting processes to obtain identification cards and birth certificates, which documents are required to register under NIIMS, are unfounded. It is their case that registration pursuant to NIIMS does not limit access to opportunities, benefits and advantages available to other members of society. They further submit that like any other citizens living on the border, the Nubians are required to undergo the vetting process. They agree with the submissions of the 2nd and 3rd Respondents that the vetting process, which the Nubians and other border communities have to undergo, has a statutory underpinning in section 8 (1) of the Act.

962. It is their case that the purpose of the vetting process is to ensure that only those with a legitimate claim to Kenyan citizenship are registered by the 4th Respondent. They further argue that the said process seeks to address the influx into the country of such communities' counterparts from neighboring countries. In their view, it is incumbent upon the 1st Petitioner to demonstrate the manner in which the vetting is discriminatory.

963. The 4th and 7th Respondents go into some details on the composition of the vetting committees. They note that they comprise an Assistant County Commissioner, a civil registration officer, an immigration officer where applicable, a chief and elders representing all communities in that locality, as well as government security agencies. They submit that the composition of these committees ensures that all communities are included in the respective Committees.

964. Like the other Respondents, the 4th and 7th Respondents maintain that equality before the law and freedom from discrimination as enshrined in Article 27 of the Constitution does not mean that every law must have universal application for all, regardless of their circumstances. It is their submission that the varying needs of different classes of persons require special treatment, and that differentiation is inherent in the concept of equality, which requires parity of treatment under parity of conditions. They cite in support the decision in **EG & 7 others v Attorney General; DKM & 9 others (Interested Parties); Katiba Institute & another (Amicus Curiae)** Petition Nos. 150 & 234 of 2016 (Consolidated).

965. They also rely on the decision of the South African Constitutional Court in **Harksen v Lane NO and Others** (CCT9/97) [1997] ZACC 12 in which the court set out the test for determining whether a claim based on unfair discrimination should succeed. Reliance is also placed on the decision in **John Harun Mwau v Independent Electoral and Boundaries Commission & Another** (supra) for the proposition that different treatment or inequality does not *per se* amount to discrimination and a violation of the Constitution. In their view, the differential treatment accorded to members of certain communities in the country serves a legitimate purpose and does not amount to unfair discrimination.

966. In his submissions on the issue of non-discrimination, the 5th Respondent submits that he understands the term ‘discrimination’ to imply any distinction, exclusion, restriction or preference which is based on any ground, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth. He relies on **Black’s Law Dictionary** which defines discrimination as:

“The effect of a law or established practice that confers privileges on a certain class or that denies privileges to a certain class because of race, age, sex, nationality, religion or handicap or differential treatment especially a failure to treat all persons equally when no reasonable distinction can be found between those favoured and those not favoured.”

967. The 5th Respondent submits that the Petitioners’ contention that the impugned amendments will result in violation of Article 27 has no basis, noting that the Petitioners have not discharged the evidentiary burden of proof. He relies on the case of **Nyarangi & 3 Others vs. Attorney General** (Supra) to submit that the law prohibits, not discrimination, but unfair discrimination.

968. With regard to the process of registration in NIIMS, the 5th Respondent argues that the only requirement for a person to be registered and issued with a unique identifying number is a national identity card. It is his case that the Respondents had provided a Data Capture Form which all Kenyans, including members of the 1st Petitioner, are required to complete. In his view, the inability of Nubians, Somalis and Arabs to provide the supporting documents as a result of extra vetting could not amount to discrimination.

969. The 5th Respondent argues that the introduction of the NIIMS database is to make the registration process much easier. His submission is that the new system will be more efficient than the current system which requires supporting documents before any identity documents are issued to the applicant. It is his case that the introduction of the NIIMS database is in no way proof of Kenyan nationality, and registration thereto does not translate to being conferred with Kenyan nationality. The 5th Respondent reiterates the purposes of NIIMs as being to create, manage, maintain and operate a national population register as a single source of

personal information of all Kenyan citizens and foreigners resident in Kenya, assign a unique national identification number on every person and to harmonize, incorporate and collate into the register, information from other databases in government agencies relating to the registration of persons.

970. In further support of his argument that there would be no discrimination as a result of the impugned amendments and the introduction of NIIMS, the 5th Respondent relies on the decision in **John Kabui Mwai & 3 Others vs. Kenya National Examination Council & 2 Others** [2011] eKLR on the form of discrimination that is prohibited by law. He submits that a claim of discrimination should be analysed from both a subjective and an objective perspective, and that in determining whether there is discrimination on grounds relating to the personal characteristics of the individual or group, the court should consider not only the impugned legislation which has created a distinction that is alleged to violate the right to equality but also to the larger social, political and legal context. The 5th Respondent also relies on the decision in **Jacques Charl Hoffmann vs. South African Airways, CCT 17 of 2000** which was cited in the High Court decision in **Centre for Rights Education and Awareness (CREAW) & 7 Others vs. Attorney General** [2011] eKLR in support of this argument. It is his position that the 1st Petitioner has failed to establish the grounds upon which the members of the Nubian community have been discriminated or even differentiated against as compared to other Kenyans. In his view, the absence of differentiation means that there is no discrimination against the Nubians and they have failed to meet the threshold set for proving the allegations of violation of the right to equality and non-discrimination.

971. The 6th Respondent also supports the position taken by the other Respondents on the issue of alleged violation of the right to equality and non-discrimination. He poses the question whether NIIMS excludes or discriminates against citizens from marginalised communities such as the Nubians. He notes that the 1st Petitioner is aggrieved that the introduction of a more complex system of registration without first addressing the challenges faced under the older, simpler system will discriminate and or exclude citizens from marginalized groups such as the Nubians who have faced difficulties in the process of registration under the current simpler system and many of them have failed to register. He notes that the 1st Petitioner has not, however, produced anything at all to support its assertion, and relies on the decision in **Mohammed Abduba Dida v Debate Media Limited & another** [2017] eKLR in which the court held that the burden lies on a person alleging unfair discrimination to establish his claim, for it is not every differentiation that amounts to discrimination.

972. It is argued on behalf of the 6th Respondent that the jurisprudence on discrimination suggests that law or conduct which promotes differentiation must have a legitimate purpose and should bear a rational connection between the differentiation and the intended purpose. Further, that the rationality requirement is intended to prevent arbitrary differentiation, and that the right to equality does not prohibit discrimination but unfair discrimination. Its submission is that in this case, there is nothing to show that NIIMS is likely to lead to discrimination against the Nubians or any other marginalized class of persons.

973. The 1st Interested Party agrees with the position taken by the Respondents that the Petitioners have failed to establish their allegations of discrimination against the members of the Nubian Community and other marginalised groups. Its submission is that the Petitioners have not set out the manner in which the impugned amendments violate any of the rights they allege violation of. In its view, there needs to be a clear manifestation of the contravention of Petition 56, 58 & 59 of 2019 (Consolidated) | Page 189 of 205.

the fundamental rights. It cites in support the decision of the Supreme Court in **Communications Commission of Kenya & 5 others v Royal Media Services Limited & 5 others** [2014] eKLR. In its view, the Petitioners' allegations of discrimination are vague, speculative and unsubstantiated, the Petitioners having failed to demonstrate the manner in which the implementation of the impugned amendments have violated any constitutional provisions.

974. The 1st Interested Party contends that all the rights which the Petitioners allege shall be infringed by the implementation of NIIMS are not absolute and can be limited, citing in support Article 25 of the Constitution. It is its contention that in considering the limitation under Article 24 (1) of the Constitution, the court must bear in mind that there are no superior rights and take into consideration factors such as the nature and extent of the limitation and the need to ensure that enjoyment of rights and fundamental freedoms by one individual does not prejudice the rights of others. Its view is that this calls for balancing of rights under the principle of proportionality because rights have equal value. Further, that the court should maintain the equality of rights as was held in the case of **University Academic Staff Union (UASU) v Attorney General & others** [2018] eKLR.

975. The 1st Interested Party further cites the case of **Attorney General & another v Randu Nzai Ruwa & 2 others** [2016] eKLR in which the Court relied on the decision by the Constitutional Court of South Africa in **Samuel Manamela & Another v The Director General of Justice CCT 25/99** for the proposition that the court must engage in a balancing exercise and arrive at a global judgment on proportionality and not adhere mechanically to a sequential check-list. Further, that as a general rule, the more serious the impact of the measure on the right, the more persuasive or compelling the justification must be.

976. It is its argument further that Article 24 of the Constitution and various judicial precedents emphasize the importance of considering the object, purpose and effect of legislation; that they require that the importance of the purpose of the limitation should be considered, as well as the relationship between the limitation and its purpose; and further, that whether there are less restrictive means of achieving the purpose should also be considered. The 1st Interested Party cites in this regard the case of **Robert Alai v The Hon Attorney General & another** [2017] eKLR in which the court observed that constitutionally guaranteed rights should not be limited except where the limitation is reasonable, justifiable and the objective of that limitation is intended to serve the society. Reliance was also placed on the Canadian case of **R. v. Oakes** [1986] 1 S.C.R. 103 in which the court stated that the onus of proving that a limitation on any Charter right is reasonable and demonstrably justified in a free and democratic society rests upon the party seeking to uphold the limitation.

977. The 1st Interested Party invites the court to take into account the fact that the government regularly rescues up to 200 children at a go, including abandoned and disabled children, who are committed to the 1st Interested Party for care and protection. The 1st Interested Party argues that it is then expected to reunite such children with their families. It is its contention that in light of such obligations placed upon it, the implementation of NIIMS is reasonable and justifiable and meets constitutional muster under Article 24 of the Constitution. Its view in this regard is on the basis that NIIMS shall ease tracing of families of separated children with special needs and the government shall be able to reunite these children with their families.

978. The 1st Interested Party further argues that NIIMS would curb cases of illicit adoption practices, child trafficking and permanent separation of children from their biological families; that NIIMS seeks to capture and store data in a centralized digital database for effective and efficient tracing of a child's family and to confirm parentage; and that the NIIMS platform will also facilitate the matching of resources to children's socio-economic needs and enable the government deliver its key constitutional mandate in accordance with its obligations under Article 53 of the Constitution.

979. Its position, therefore, is that NIIMS is reasonable, proportionate and justifiable in an open and democratic society when the the plight of Kenyan children, whose rights are protected under Article 53 of the Constitution, is considered.

980. The 8th and 9th Interested Parties also discount the argument that NIIMS will lead to violation of the Petitioners' rights under Article 27 of the Constitution. They submit, through their Learned Counsel, Mr. Omuganda, who highlighted their submissions dated 14th October, 2019 that the Constitution contemplates limitation of the rights and fundamental freedoms, and the greater public interest and security concerns far outweigh individual rights. It is their position that Article 24(1) of the Constitution permits limitation of rights if the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. Their view is that the rights to privacy, equality and non-discrimination fall within the purview of rights that can be limited for security reasons.

981. From the respective submissions of the parties set out above, it appears to us that there are two facets of the alleged denial of the right to equality and non-discrimination disclosed. The first relates to the argument, advanced by the 1st Petitioner and supported by the 2nd Petitioner and the 5th Interested Party, that the impugned amendments and the implementation of NIIMS will perpetuate discrimination against members of the Nubian community and other marginalised groups. The second relates to the contention that the impugned law makes it mandatory for everyone to obtain a *Huduma Namba*, failing which one will be denied Government services.

On Discrimination of the Nubian Community

982. The starting point in considering this issue is to look at the law and previous jurisprudence with regard to discrimination. So far as is relevant for present purposes, Article 27 of the Constitution guarantees to everyone the right to equality and non-discrimination in the following terms:

27. (1) Every person is equal before the law and has the right to equal protection and equal benefit of the law.

(2) Equality includes the full and equal enjoyment of all rights and fundamental freedoms.

(3)...

(4) The State shall not discriminate directly or indirectly against any person on any ground, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth.

(5) ...

983. The precise meaning and implication of the right to equality and non-discrimination has been the subject of numerous judicial decisions in this and other jurisdictions. In its decision in **Jacqueline Okeyo Manani & 5 Others v. Attorney General & Another** (supra) the High Court stated as follows with respect to what amounts to discrimination:

“26. Black’s Law Dictionary, 9th Edition defines “discrimination” as (1) “the effect of a law or established practice that confers privileges on a certain class because of race, age sex, nationality, religion or hardship” (2) “Differential treatment especially a failure to treat all persons equally when no reasonable distinction can be found between those favoured and those not favoured”.

27. In the case of *Peter K Waweru v Republic* [2006]eKLR, the court stated of discrimination thus:-

“Discrimination means affording different treatment to different persons attributable wholly or mainly to their descriptions whereby persons of one such description are subjected to ... restrictions to which persons of another description are not made subject or have accorded privileges or advantages which are not accorded to persons of another such description... Discrimination also means unfair treatment or denial of normal privileges to persons because of their race, age sex ... a failure to treat all persons equally where no reasonable distinction can be found between those favoured and those not favoured.”(emphasis)

28. From the above definition, discrimination, simply put, is any distinction, exclusion or preference made on the basis of differences to persons or group of persons based such considerations as race, colour, sex, religious beliefs political persuasion or any such attributes that has real or potential effect of nullifying or impairing equality of opportunity or treatment between two persons or groups. Article 27 of the Constitution prohibits any form of discrimination stating that. (1) Every person is equal before the law and has the right to equal protection and equal benefit of the law, and that (2) Equality includes the full and equal enjoyment of all rights and fundamental freedoms.

29. The Constitution advocates for non-discrimination as a fundamental right which guarantees that people in equal circumstances be treated or dealt with equally both in law and practice without unreasonable distinction or differentiation. It must however be borne in mind that it is not every distinction or differentiation in treatment that amounts to discrimination. Discrimination as seen from the definitions, will be deemed to arise where equal classes of people are subjected to different treatment, without objective or reasonable justification or proportionality between the aim sought and the means employed to achieve that aim.

30. In this regard, the Court stated in the case of *Nyarangi & 3 Others V Attorney General* [2008] KLR 688 referring to the repealed constitution; “discrimination that is forbidden by the constitution involves an element of unfavourable bias. Thus, firstly unfavourable bias must be shown by the complainant; and secondly, the bias must be based on the grounds set in the

constitutional definition of the word “discriminatory” in section 82 of the Constitution.”

984. It is thus recognised that it is lawful to accord different treatment to different categories of persons if the circumstances so dictate. Such differentiation, however, does not amount to the discrimination that is prohibited by the Constitution. In **John Harun Mwau v. Independent Electoral and Boundaries Commission & Another** (supra), the court observed that:

“[i]t must be clear that a person alleging a violation of Article 27 of the Constitution must establish that because of the distinction made between the claimant and others, the claimant has been denied equal protection or benefit of the law. It does not necessarily mean that different treatment or inequality will per se amount to discrimination and a violation of the constitution.”

985. When faced with a contention that there is a differentiation in legislation and that such differentiation is discriminatory, what the court has to consider is whether the law does indeed differentiate between different persons; if it does, whether such differentiation amounts to discrimination, and whether such discrimination is unfair. In **EG & 7 others v Attorney General; DKM & 9 others (Interested Parties); Katiba Institute & Another: Petition 150 & 234 of 2016 (Consolidated)** the court held that:

“[288]. 288. From the above definition, it is safe to state that the Constitution only prohibits unfair discrimination. In our view, unfair discrimination is differential treatment that is demeaning. This happens when a law or conduct, for no good reason, treats some people as inferior or less deserving of respect than others. It also occurs when a law or conduct perpetuates or does nothing to remedy existing disadvantages and marginalization.”

986. In **Harksen v Lane NO and Others** (supra) the Court observed that the test for determining whether a claim based on unfair discrimination should succeed was as follows:

(a) Does the provision differentiate between people or categories of people" If so, does the differentiation bear a rational connection to a legitimate purpose" If it does not, then there is a violation of the constitution. Even if it does bear a rational connection, it might nevertheless amount to discrimination.

(b) Does the differentiation amount to unfair discrimination" This requires a two-stage analysis: -

(i) Firstly, does the differentiation amount to ‘discrimination’" If it is on a specified ground, then discrimination will have been established. If it is not on a specified ground, then whether or not there is discrimination will depend upon whether, objectively, the ground is based on attributes and characteristics which have the potential to impair the fundamental human dignity of persons as human beings or to affect them adversely in a comparably serious manner.

(ii) If the differentiation amounts to ‘discrimination,’ does it amount to ‘unfair discrimination?’ If it has been found to have been on a specified ground, then the unfairness will be presumed. If on an unspecified ground, unfairness will have to be established by the complainant. The test of unfairness focuses primarily on the impact of the discrimination on the complainant and others in his or her situation. If, at the end of this stage of the enquiry, the differentiation is found not to be unfair, then there will be no violation...

(c) If the discrimination is found to be unfair then a determination will have to be made as to whether the provision can be justified under the limitations clause.

987. With respect to the burden of proof on a claim that an action or law is discriminatory, it has been held that the burden lies on a person alleging unfair discrimination to establish his claim. In Mohammed Abduba Dida v Debate Media Limited & another [2017] eKLR, the court (Mativo J) stated as follows:

“I must add that if the discrimination is based on any of the listed grounds in Article 27 (4) of the Constitution, it is presumed to be unfair. It must be noted, however, that once an allegation of unfair discrimination based on any of the listed grounds in article 27 (4) of the constitution is made and established, the burden lies on the Respondent to prove that such discrimination did not take place or that it is justified.

On the other hand, where discrimination is alleged on an arbitrary ground, the burden is on the complainant to prove that the conduct complained of is not rational, that it amounts to discrimination and that the discrimination is unfair.”

988. It must also be noted, as observed by Mativo J in Mohammed Abduba Dida v Debate Media Limited & another (supra) that:

“It is not every differentiation that amounts to discrimination. Consequently, it is always necessary to identify the criteria that separate legitimate differentiation from constitutionally impermissible differentiation. Put differently, differentiation is permissible if it does not constitute unfair discrimination.”

989. Turning to the facts of the present matter, we pose the questions: does the impugned amendment differentiate between members of the Nubian community and other marginalised groups and other Kenyans" If it does, does it have a rational basis and is it therefore constitutionally permissible"

990. Section 9A(1) of the impugned Act established the “National Integrated Identity Management System” whose function is “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”. The impugned law thus applies to all persons resident in Kenya, whether nationals or citizens of other states. To that extent, the law as enacted does not differentiate between nationals or foreigners, and thus everyone, including members of the Nubian community and other groups such as members of the Shona community who are citizens of or resident in Kenya, are entitled to register. Indeed, the 1st Petition 56, 58 & 59 of 2019 (Consolidated) | Page 194 of 205.

Petitioner and its witnesses acknowledge that they are entitled to register for the *Huduma Namba*.

991. Their challenge to the system is that they encounter challenges and hardships in acquiring identity documents under the existing system, particularly the vetting process mandated under section 8(1A) of the Act. They assert that the Act grants registration officers broad authority to demand additional evidence from persons from marginalized areas, and they are faced with an onerous process of establishing their Kenyan nationality in order to obtain identity cards. The gist of their grievance, as we understand it, is that the vetting process that they are subjected to under section 8(1A) of the Act is discriminatory and therefore a violation of their rights under Article 27.

992. We have set out above the responses of the Respondents to these contentions, and we are constrained to agree with them that the Petitioners have not established a violation of the right to equality and non-discrimination. First, the law that established NIIMS, as submitted by the Respondents, does not establish or require that one undergoes a vetting process. As we understand the law to be, one has to present themselves with an identity document issued under a different piece of legislation in order to be registered under NIIMS.

993. In the case of foreign nationals, refugees and stateless persons, the legislation under which identity documents will continue to be issued are the Kenya Citizenship and Immigration Act and the Refugee Act. Whatever the conditions for issuance of identity documents are under these Acts must be met before one is issued with an appropriate identity document, subsequent to which one may present the said document in order to register with NIIMS. In the case of Kenyan nationals, as we understand it, the issuance of identity documents will continue under the existing system of law: certificates of birth under the Births and Deaths Registration Act, and for national identity cards, the Registration of Persons Act.

994. It was deposed and submitted by the 2nd and 3rd Respondents, and not controverted by the Petitioners, that the requirement for vetting of persons from border communities was introduced to section 8(1A) of the Act by the Security Laws (Amendment) Act, No 19 of 2014. This section provides as follows:

“1A) The Director may establish identification committees or appoint persons as identification agents to assist in the authentication of information furnished by a parent or guardian.

995. As submitted by the Respondents, this provision of the Act was not introduced by the impugned law, nor is it under challenge in the Consolidated Petitions before us. Indeed, it was not one of the provisions that was challenged in the consolidated petitions that impugned the process and substance of the Security Laws (Amendment) Act of 2014 that was the subject of determination in **Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others (Supra)**. We do not, therefore, have before us legislation that contains a differentiation between members of the Nubian community and other marginalised groups as compared with other Kenyans. What we have is an amendment to an existing statute that introduces a system of registration into the population register that requires that one should be in possession of identification documents issued under other statutory provisions. It seems to us that should there be challenges with those other statutes or specific statutory provisions and the conditions for issuance of identity documents under the said statutes, then such challenges

and conditions cannot properly be challenged in the present proceedings in which the statutory provisions in contention are entirely different.

996. Even had we found that there is legislation that contains differentiation between members of the Nubian and other communities and other groups in Kenya, there is yet another hurdle that the Petitioners would need to surmount. This is the question whether the Petitioners have laid a factual basis for the allegation that there is violation of the right to equality and non-discrimination of the Nubians and other marginalised communities. As held in the Anarita Karimi Njeru Case and Trusted Society for Human Rights Case (supra), the Petitioners have an obligation to show how the right to equality and non-discrimination has been violated by the State. This would require, as submitted by the 1st Respondent, that there should be evidence from members of the communities alleged to be discriminated against that demonstrates how the NIIMS process, or indeed the vetting process under section 8(1)(A) of the Registration of Persons Act is conducted in a manner that is violative of their rights. What is the evidence presented before us"

997. PW3, Ahmed Khalil Kafe, is a Kenyan citizen of Nubian descent born on 18th March 1946. He served as a police officer from 1965 to 1972. At around the time he retired from the Police Force in 1972, he lost his identification card, a driving licence and police card. He obtained a police abstract, but the abstract in time became worn out and eventually all the writings on it disappeared. He applied for replacement of his national identification card on 19th November 2018.

998. During the verification process for replacement of his identification card, he was informed that his fingerprints were not available in the records at the National Registration Bureau and was asked to swear an affidavit to facilitate the replacement of the national identification card. His testimony was that it has been four years since he lost his documents and his efforts to replace them were fruitless. He had applied for a *Huduma Namba* on 10th April 2019 but the officials had sent him away without attending to him. He stated, however, that he had a waiting card issued to him on 5th September 2019. He stated that his problem in this case is that without an identity card he cannot get a *Huduma Namba*.

999. The affidavit and oral evidence of Mr. Shafi Ali Hussein, in so far as it relates to the alleged discrimination against members of the Nubian community and other marginalised groups, was primarily directed at the vetting process and the composition of the vetting committees established under section 8(1A) of the Act. He contended that while vetting is intended to counteract fraudulent acquisition of documents, it was not applied to other ethnic groups. Mr. Hussein conceded, somewhat reluctantly, that he had written the letter of appreciation dated 8th April 2017 to the National Registration Bureau. The letter had been written on behalf of the 1st Petitioner which was partnering with the Registrar of Persons in mobilising residents in the issuance of identity cards and birth certificates.

1000. Ms. Fatuma Abdirahman's testimony traces the challenges faced by Nubians to the 1990s, their quest for the Kibra land, and the 1998 bombing of the American embassy. Prior to 1990, the Nubian community had accessed identity documents like other Kenyans, but since then the community was subjected to differential treatment with regard to accessing birth certificates, national identity cards, and passports. The security vetting had intensified after the process was legalised by the Security Laws (Amendment) Act of 2014.

1001. Ms. Abdirahman narrated the steps taken by the 1st Petitioner to improve access to government documentation for members of the Nubian community, testifying that over 3,200
Petition 56, 58 & 59 of 2019 (Consolidated) | Page 196 of 205.

people had been assisted to apply for birth certificates, identity cards, passports, and death certificates. She was aggrieved that Nubians in Kibra are only able to apply for identity cards on Tuesdays or Thursdays, the days on which the vetting committees sit.

1002. Taken together, and with the greatest respect to the 1st Petitioner, we are unable to discern violation of the right to equality and non-discrimination from the evidence presented before us. What we have is the evidence of one witness who had obtained identification documents issued as far back as 1961, lost them in 1972, obtained a police abstract but did not follow up on it and the writings on it faded; and only applied for a replacement identification card in November 2018, 46 years after he lost the documents. His evidence, we must observe, was quite inconsistent and not quite reliable, and is not demonstrative of the alleged challenges and discrimination.

1003. The other evidence indicates that the 1st Petitioner has been able to enter into partnerships with State agencies such as the National Registration Bureau and mobilised residents to get identification cards as well as births and deaths certificates. Contrary to the assertions of Mr. Hussein, the letter of 8th April 2017 is more suggestive of a community that is happy with the manner in which the issuance of documents was progressing. All in all, we are unable to find a basis for faulting the impugned amendments on the basis that they had resulted in violation of the right to equality and non-discrimination.

On Exclusion

1004. The Petitioners have contended that the impugned amendments make it mandatory to register under NIIMS and to obtain the unique identification number. They are aggrieved that under section 9A(2)(d), NIIMS shall, among other things, support the printing and distribution of all identification documents in the country. They are further aggrieved that public services connected to these identification documents will only be offered to those who surrender their personal biometric information and are issued with the *Huduma Namba*. This contention requires that we address ourselves to the question whether obtaining the *Huduma Namba* is mandatory, a condition precedent to obtaining government services, and therefore likely to result in exclusion and violation of the right to non-discrimination.

1005. The parties to this matter have not addressed themselves to this issue in their submissions. However, it emerges as a core grievance of the Petitioners in the affidavit evidence of Ms. Munyua and Mr. Kegoro, and the oral testimony of Mr. Hussein. Ms. Munyua averred that the NIIMS process should not be used for exclusion. While noting that possessing an identity is increasingly a precondition to accessing basic services, and since vital government services will require a *Huduma Namba*, she averred that there was the potential for excluding from the system those who may not have registered for various reasons.

1006. The position taken by the Petitioners is that care should be taken not to exclude anyone from the identification system because of their physical, social, demographic, or economic characteristics. Ms. Munyua noted in particular the potential to exclude marginalized communities since officials will be using existing documents to verify who is a citizen, thus locking out people who do not have these identification documents such as the Makonde, the Shona and pastoral communities.

1007. George Kegoro makes similar averments with regard to the potential for NIIMS to result in exclusion and consequent denial of government services if such services are pegged

on registration in NIIMS and possession of the *Huduma Namba*, a result that would be inconsistent with Article 12(2) which relates to citizenship rights, and Article 24 of the Constitution.

1008. The Respondents counter that registration under NIIMS is meant to be an ongoing exercise. Dr. Kibicho averred that it will not be discontinued at the lapse of 45 days of mass registration. Their contention is that there is no danger of exclusion as deserving persons who do not currently have the requisite identification documents can obtain them within the parameters set by the law and thereafter register for the *Huduma Namba*.

1009. On his part, Jerome Ochieng sees advantages in the NIIMS system over the current registration system. He avers that the current registration system has some shortcomings, including access to documents or access to the registration system. He illustrates this by noting that under the current system, applicants for national identity cards are required to produce their birth certificates and their parents' national identity cards, among others. In the Respondents' view, with registration in NIIMS, all this information shall be captured and there will thus be no need for such documentation. The argument from the Respondents thus posits that NIIMS will reduce the duplication of processes common in accessing government services as it will serve as a one-stop shop for identification information, thus rendering access to government more efficient.

1010. We have two scenarios presented to us by the parties with respect to the consequences of the implementation of NIIMS. The first is the gloomy scenario that the Petitioners fear will lead to the exclusion of significant portions of the population from accessing government services on account of a failure to register under NIIMS. Such a failure may result from a choice, an election, not to surrender vital personal data to the system, or from the inability to register due to the lack of personal identification documents as may happen, according to the Petitioners, with respect to marginalised communities.

1011. Then there is the optimistic scenario painted by the Respondents in which access to government services will be easy and efficient as all the personal data will be available within the NIIMS system and accessible at the click of a mouse. A consideration of the issue of exclusion requires that we try to find a balance and arrive at an approximation of where the truth between these two divergent scenarios lies, and to arrive at a determination that will advance the rights of citizens and all others resident within the borders of Kenya who require government services.

1012. We note that all the parties are agreed that the use of digital data is the way of the future. The challenge is to ensure, among other things, that no one is excluded from the NIIMS and the attendant services. This may occur due to lack of identity documents, or lack of or poor biometric data, such as fingerprints. In our view, there may be a segment of the population who run the risk of exclusion for the reasons already identified in this judgment. There is thus a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS. Suffice to say that while we recognize the possibility of this exclusion, we find that it is in itself not a sufficient reason to find NIIMS unconstitutional.

Whether the 1st Petitioner's Petition is barred by the Principles of Sub Judice Res Judicata

1013. A final, corollary issue raised against the 1st Petitioner's case is that its Petition offends the principles of *sub-judice* and *res judicata*. The 2nd and 3rd Respondents submit that the 1st Petitioner is precluded from reviving the Nubian community cases in the present Petition by the doctrine of *sub judice*. They submit that the issues raised by the 1st Petitioner in this matter were previously litigated before the High Court. It is their contention that in the Nubian Community case before the African Commission, the Nubian Community, which was the complainant, noted that it had instructed the Center for Minority Rights Development to institute a suit against the government of Kenya for denial of citizenship and for discrimination in the issuance of identity documents.

1014. While noting that the 1st Petitioner has not proved to the court whether that petition, which was filed on 17th March 2003 and referred to in the Nubian Community case, was decided, it is their submission that the 1st Petitioner is nonetheless barred by the doctrine of *sub judice* from litigating on issues which had been previously raised in a petition before this Court. The 2nd and 3rd Respondents rely on section 6 of the Civil Procedure Act and the decision in **Edward R. Ouko v Speaker of the National Assembly & 4 others** [2017] eKLR in which the High Court set out the principles to be considered in order to find that the doctrine was applicable. These principles, according to the 2nd and 3rd Respondents, are first, that there must exist two or more suits filed consecutively; that the matter in issue in the suits or proceedings must be directly and substantially the same; that the parties in the suits or proceedings must be the same or must be parties under whom they or any of them claim, litigating under the same title; and the suits must be pending in the same or any other court having jurisdiction in Kenya to grant the relief claimed.

1015. It is their submission that the above principles apply with respect to the present petition by the 1st Petitioner. They assert that both petitions filed by the Nubian Community seek to enforce their right to citizenship and non-discrimination under the Constitution; that both claims are directed against the government and the Ministry of Interior and Co-ordination of the National Government and Security through the Attorney General; and that both petitions were instituted either by the 1st Petitioner acting in its own capacity or through a non-governmental organization as in the first petition.

1016. It is also the 2nd and 3rd Respondents' submission, in the alternative, that the 1st Petitioner's claim in the present petition is barred by the doctrine of *res judicata*. They submit that in the event that it is proved that the earlier petition filed in the High Court was determined, then the 1st Petitioner is barred from re-litigating the same issue on the basis of the doctrine of *res judicata* set out in section 7 of the Civil Procedure Act and explanation 3 thereof. They rely in support of this submission on the decision in **Independent Electoral and Boundaries Commission v Maina Kiai & 5 others, Nairobi** ([2017] eKLR) in which the Court of Appeal noted that:

“.....for the bar of res judicata to be effectively raised and upheld on account of a former suit, the following elements must be satisfied, as they are rendered not in disjunctive but conjunctive terms;

(a) The suit or issue was directly and substantially in issue in the former suit.

(b) That former suit was between the same parties or parties under whom they or any of them claim.

(c) *Those parties were litigating under the same title.*

(d) *The issue was heard and finally determined in the former suit.*

(e) *The court that formerly heard and determined the issue was competent to try the subsequent suit or the suit in which the issue is raised.”*

1017. They further cite the words of the Court in the said decision in which it stated that:

(f) *“The rule or doctrine of res judicata serves the salutary aim of bringing finality to litigation and affords parties closure and respite from the spectra of being vexed, haunted and hounded by issues and suits that have already been determined by a competent court. It is designed as a pragmatic and commonsensical protection against wastage of time and resources in an endless round of litigation at the behest of intrepid pleaders hoping, by a multiplicity of suits and fora, to obtain at last, outcomes favorable to themselves. Without it, there would be no end to litigation, and the judicial process would be rendered a noisome nuisance and brought to disrepute or calumny. The foundations of res judicata thus rest in the public interest for swift, sure and certain justice.”* (Emphasis added)

1018. The 2nd and 3rd Respondents allege bad faith on the part of the 1st Petitioner and urge the Court to note the bad faith it exhibits in instituting two similar suits before this Court and other suits outside the jurisdiction, actions which they term abuse of process. The 1st Petitioner did not respond to these arguments.

1019. We have considered this issue and the submissions made by the 2nd and 3rd Respondents, which have not been countered by the 1st Petitioner. There is no material before us to indicate whether or not the suit filed in the High Court alleging violation of the rights of the Nubians has been determined, and if so, what the outcome thereof was. It would appear, however, that as argued by the 2nd and 3rd Respondents, the issue of alleged violation of the rights of members of the Nubian community has been under consideration by a court of concurrent jurisdiction and has been determined or is pending determination.

1020. We also have before us the decision in **Institute for Human Rights & Development in Africa & Open Society Justice Initiative on behalf of Children of Nubian descent in Kenya v Kenya**, Communication no. Comm/002/2009 of March 2011 in which the African Committee of Experts on the Rights and Welfare of the Child (ACERWC) found that the Republic of Kenya had violated the rights of children of Nubian descent under the African Charter on the Rights and Welfare of the child, which explicitly recognizes the right to a nationality. It would appear to us, therefore, that the 1st Petitioner is indeed raising issues that have been the subject of judicial interpretation or are pending interpretation in our courts.

1021. However, the issues before us arise in the context of the constitutionality of the amendments to the Registration of Persons Act. As was held by the Court of Appeal in the case of **John Florence Maritime Services Limited & Another vs Cabinet Secretary for Transport and Infrastructure and 3 Others**, (2015) eKLR the doctrine of *res judicata* must be sparingly invoked with regard to constitutional petitions, for the reason that rights keep on evolving, mutating and assuming multifaceted dimensions. We therefore decline to find that the 1st Petitioner’s Petition is *res-judicata*.

Summary of Findings

1022. Arising from our findings in the foregoing sections, it is our view that the Petitions partially succeed to the extent already stated in the judgment. We set out below a summary of our findings.

On Whether the Legislative Process was Constitutional

1023. In addressing this issue we considered whether the impugned amendments were subjected to public participation in accordance with the Constitution, whether the enactment by way of an omnibus Statute Law (Miscellaneous Amendment) Act was procedural or appropriate in the circumstances, and finally, whether the impugned law was a Bill concerning counties and should therefore have been subjected to approval of the Senate.

1024. All the parties were agreed that public participation is a key element in the achievement of democratic governance and is a constitutional imperative. Our view is that the time that was available for public participation must be considered in light of all the processes of the legislative process. In the present Petition, the evidence before us suggests that the public was aware of the Bill from 10th April 2018, when it was published, and could have participated from that date until the committee hearings on 14th, 19th and 20th June 2018. The evidence from the Respondent demonstrated that this opportunity was given to the public, and that indeed there was participation by the 3rd Petitioner even after expiry of the time stated in the advertisement. It was thus our finding that sufficient time was afforded for public participation on the enactment of Statute Law (Miscellaneous Amendments) Act 2018.

1025. We also took the view that whenever the issue of the use of an omnibus Bill arises, the question to be posed is whether the procedure has, in the circumstances of the particular case, limited the right of the public to participate in the legislature's business. However, if there is evidence placed before the court by the legislature to demonstrate that the principle of public participation was complied with in the process of the amendments, then the court should not be quick to hold such amendments invalid simply because an omnibus Bill was used to make the amendments.

1026. We noted that it is not in the place of the courts to dictate the procedures to be used by the two houses of Parliament in executing their legislative mandate. The business of the court is to confirm that the legislative bodies have complied with the Constitution and the law in delivering on their mandates. In this respect, as we had already found that there was evidence of sufficient time for public participation, and the procedure employed by the 6th Respondent in the stakeholder engagement of the Omnibus Bill during the Committee Stage by various Committee did facilitate public participation, we did not find the use of the omnibus Bill in the enactment of Statute Law (Miscellaneous Amendments) Act 2018 unconstitutional.

1027. On whether the Bill was a Bill concerning counties, we were of the view that the jurisdiction of the Senate does not extend to each and every legislation passed by the National Assembly, and that to hold so would render Article 110 of the Constitution redundant. In addition, while the Fourth Schedule of the Constitution does indeed give a wide array of functions to the counties, in our view, these functions do not include creation and maintenance of a national population register. It was therefore our finding and holding that the enactment of the impugned amendments did not require the involvement of the Senate.

Whether there is Violation and/or Threatened Violation of the Right to Privacy.

(a) Whether the personal information collected is excessive, intrusive, and disproportionate.

1028. There were two limbs of arguments raised as regards this issue. The first limb was that the provisions for collection of biometric data by the impugned amendments was intrusive and unnecessary. Closely related to the first limb of the issue at hand is the second limb that the data collected pursuant to the impugned amendments is not supported by the stated purposes of NIIMS and is purpose free.

1029. We considered in this regard the scope and content of the right to privacy including information, and found that biometric data and GPS coordinates required by the impugned amendments are personal, sensitive and intrusive data that requires protection. Even though there was no evidence brought by the Petitioners of any violations of rights to privacy in this respect, we also found that the impugned amendments impose an obligations on the relevant Respondents to put in place measures to protect the personal data.

1030. It was also our holding that the biometric data collected is necessary to the stated purposes of NIIMS in section 9A of the Registration of Persons Act, and the functionalities of NIIMS as an identification and verification system in our view, also justified the utility of NIIMS and the other existing identification and registration databases. It was thus our finding that NIIMS is not superfluous from an identification and verification point of view, as the biometric data collected therein is necessary for identification, and will be used for verification purposes in relation to other existing databases. Lastly, we found the stated benefits of NIIMS given by the Respondents in their evidence to be in the public interest and not unconstitutional.

(b) Whether there is a Violation of Children's Right to Privacy

1031. It was evident that the provisions of section 9A of the Registration of Persons Act on the purposes of NIIMS contradict section 2, and the two provisions cannot operate at the same time with regard to the application of NIIMS to children. After applying the rules of statutory interpretation on implied amendment and repeal detailed out in the judgment, it is our finding that section 9A, being a later amendment, is deemed to have amended section 2 with respect to its application to NIIMS, and to this extent the inconsistency was thereby resolved. We therefore found that section 9A of the Registration of Persons Act and NIIMS applies to children.

1032. We were also of the view and found that the general principles and protections that apply with regard to the right to informational privacy, and our findings in this regard with respect to the biometric data collected under NIIMS are also applicable to children, as much as they apply to adults, and even more. This is because unlike adults, children's ability to make reasonable choices about what information to share is limited, as a result of their limited capacities, development and education. The additional issue which we therefore considered was whether the impugned amendments and NIIMS provide specific protection with regard to children's personal data.

1033. In this regard we noted some gaps in the Data Protection Act, namely that there is no definition of a child in the Act, and the rights of the child in relation to the data so collected during minority and majority stages are also not specified, particularly in light of their evolving capacities and best interests. In addition, despite NIIMS being applicable to children, there are no special provisions in the impugned amendments, and no regulations that govern how the data relating to children is to be collected, processed and stored in NIIMS. It was our conclusion therefore that the legislative framework on the protection of children's biometric data collected in NIIMS is inadequate.

(c) Whether there are Sufficient Legal Safeguards and Data Protection Frameworks

1034. We noted that the protection of personal data depends largely on a legal, regulatory and institutional framework that provides for adequate safeguards, including effective oversight mechanisms. This is especially the case with NIIMS, whereby a vast amount of personal data is accessible to The State, and data subjects currently have limited insight into and control over how information about them and their lives is being used.

1035. While we found that the Data Protection Act No 24 of 2019 has included most of the applicable data protection principles, we noted that there are a number of areas in the Act that require to be operationalised by way of regulations, including circumstances when the Data Commissioner may exempt the operation of the Act, and may issue data sharing codes on the exchange of personal data between government departments. It is our view that these regulations are necessary, as they will have implications on the protection and security of personal data.

1036. We also observed that once in force, data protection legislation must also be accompanied by effective implementation and enforcement. The implementation of the Data Protection Act 24 of 2019 requires an implementation framework to be in place, including the appointment of the Data Commissioner, and registration of the data controllers and processors, as well as enactment of operational regulations. It was our finding therefore that while there is in existence a legal framework on the collection and processing of personal data, adequate protection of the data requires the operationalisation of the said legal framework.

1037. On the safety and security concerns raised related to the design of NIIMS, it was our conclusion that all biometric systems, whether centralised or decentralised, and whether using closed or open source technology, require a strong security policy and detailed procedures on its protection and security which comply with international standards. For our purposes, what was relevant is that the said principles and standards should be provided and actualized in regulations that will govern the operation of NIIMS. In addition, it was our view that the biometric data and personal data in NIIMS should only be processed if there is an appropriate legal framework in which sufficient safeguards are built in to protect fundamental rights.

1038. In this respect, while the Respondents explained the measures they have put in place to ensure the safety of the data collected by NIIMS and the security of the system, including the encryption of the data and restricted access, it was not disputed by the Respondents that there is no specific regulatory framework that governs the operations and security of NIIMS. The Respondents also did not provide any cogent reason for this obvious gap. To this extent we found that the legal framework on the operations of NIIMS is inadequate, and poses a risk to the security of data that will be collected in the system.

(d) Whether the Impugned Amendments are an Unnecessary, Unreasonable and Unjustifiable Limitation.

1039. It was our finding that because of the specificity of the information that DNA may disclose and the harm disclosure may cause not just to the data subject but other family members in terms of both identification and genetic information, DNA information requires and justifies a particular and specific legal protection. Likewise, we found that specific authorization anchored in law is required for the use of GPS coordinates in light of the privacy risks we identified in terms of their possible use to track and identify a person's

location. Accordingly, we found that the provision for collection of DNA and GPS coordinates in the impugned amendments, without specific legislation detailing out the appropriate safeguards and procedures in the said collection, and the manner and extent that the right to privacy will be limited in this regard, is not justifiable.

1040. We also noted that an inadequate legislative framework for the protection and security of the data is clearly a limitation to the right to privacy in light of the risks it invites for unauthorized access and other data breaches. To this extent we found the lack of a comprehensive legislative framework when collecting personal data under the impugned amendments, is contrary to the principles of democratic governance and the rule of law, and thereby unjustifiable.

Whether there was a Violation of the Right to Equality and Non-Discrimination

1041. There were two facets of the alleged denial of the right to equality and non-discrimination disclosed. The first relates to the argument that the impugned amendments and the implementation of NIIMS will perpetuate discrimination against members of the Nubian community and other marginalised groups. The second relates to the contention that the impugned law makes it mandatory for everyone to obtain a *Huduma Namba*, failing which one will be denied government services.

(a) On Discrimination against the Nubian Community

1042. We found that the impugned legislation did not contain a differentiation between members of the Nubian community and other marginalised groups as compared with other Kenyans. What we found is an amendment to an existing statute that introduces a system of registration into the population register that requires that one should be in possession of identification documents issued under other statutes or statutory provisions. It was our view that should there be challenges with those other statutes or provisions, then such challenges cannot properly be raised in the present proceedings in which the legislation or provision in contention is entirely different.

1043. We also considered the question whether the Petitioners had laid a factual basis for the allegation that there is violation of the right to equality and non-discrimination against the Nubians and other marginalised communities. We were unable to discern violation of the right to equality and non-discrimination from the evidence presented before us.

(b) On Exclusion

1044. We addressed ourselves to the question whether obtaining the *Huduma Namba* is mandatory, a condition precedent to obtaining government services, and therefore likely to result in violation of the right to non-discrimination. We noted that all the parties were agreed that the use of digital data is the way of the future. The challenge is to ensure among other things, that no one is excluded from the NIIMS and the attendant services. This may occur due to lack of identity documents, or lack of or poor biometric data, such as fingerprints. In our view there may be a segment of the population who run the risk of exclusion.

1045. We therefore found that there is thus a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS. While we recognize the possibility of this exclusion, however, we did not find that it is in itself a sufficient reason to find NIIMS unconstitutional.

Cost

1046. The final issue to consider is who should bear the costs of the consolidated Petitions. The applicable principles are that costs follow the event. However, the award of the costs is also at the discretion of the Court. As this is a matter which clearly raises public interest concerns, it is our view that each party shall bear its own costs.

Disposition

1047. In light of our findings above, we hereby grant, the following orders:

I. A declaration that the collection of DNA and GPS co-ordinates for purposes of identification is intrusive and unnecessary, and to the extent that it is not authorised and specifically anchored in empowering legislation, it is unconstitutional and a violation of Article 31 of the Constitution.

II. Consequently, in so far as section 5(1)(g) and 5(1)(ha) of the Registration of Persons Act requires the collection of GPS coordinates and DNA, the said subsections are in conflict with Article 31 of the Constitution and are to that extent unconstitutional, null and void.

III. The Respondents are at liberty to proceed with the implementation of the National Integrated Identity Management System (NIIMS) and to process and utilize the data collected in NIIMS, only on condition that an appropriate and comprehensive regulatory framework on the implementation of NIIMS that is compliant with the applicable constitutional requirements identified in this judgment is first enacted.

IV. Each party shall bear its own costs of the Consolidated Petitions

1048. Orders accordingly.

DATED, SIGNED AND DELIVERED AT NAIROBI THIS 30TH DAY OF JANUARY 2020.

P. NYAMWEYA

MUMBI NGUGI

W. KORIR

JUDGE

JUDGE

JUDGE



While the design, structure and metadata of the Case Search database are licensed by [Kenya Law](#) under a [Creative Commons Attribution-ShareAlike 4.0 International](#), the texts of the judicial opinions contained in it are in the [public domain](#) and are free from any copyright restrictions. Read our [Privacy Policy](#) | [Disclaimer](#)