Katiba Institute v Communications Authority of Kenya & 2 others; Data Privacy and Governance Society of Kenya & 3 others (Interested Parties); Ideate Policy Africa Limited (ITPA) (Amicus Curiae) (Petition E647 of 2024) [2025] KEHC 10568 (KLR) (Constitutional and Human Rights) (18 July 2025) (Judgment)

Neutral citation: [2025] KEHC 10568 (KLR)

REPUBLIC OF KENYA

IN THE HIGH COURT AT NAIROBI (MILIMANI LAW COURTS)

CONSTITUTIONAL AND HUMAN RIGHTS

PETITION E647 OF 2024

EC MWITA, J

JULY 18, 2025

BETWEEN

KATIBA INSTITUTE ..... PETITIONER

AND

COMMUNICATIONS AUTHORITY OF KENYA ..... 1ST RESPONDENT

KENYA REVENUE AUTHORITY ..... 2ND RESPONDENT

ATTORNEY GENERAL ..... 3RD RESPONDENT

AND

DATA PRIVACY AND GOVERNANCE SOCIETY OF KENYA .... INTERESTED PARTY

INTERNATIONAL COMMISSION OF JURISTS (KENYA) .... INTERESTED PARTY

LAW SOCIETY OF KENYA ..... INTERESTED PARTY

THE CONSUMERS FEDERATION OF KENYA (THROUGH EPHRAIM KANAKE, STEPHEN MUTORO AND HENRY OCHIENG) ..... INTERESTED PARTY

AND

IDEATE POLICY AFRICA LIMITED (ITPA) ..... AMICUS CURIAE

JUDGMENT

Background

1. On 24th October 2024, the 1st respondent issued a public notice through its official X account and website titled "Public Notice on Enhancing the Integrity and Tax Compliance of the Mobile Devices in Kenya." The notice was to notify all stakeholders, including mobile network operators involved in local assembly, importation, distribution and connection of mobile devices to the local networks, of new requirements that were to take effect on 1st January 2025.

2. The notice required all local device assemblers to upload International Mobile Equipment Identity (IMEI) Numbers of each assembled device to the Kenya Revenue Authority(KRA) Portal; all mobile phone importers to disclose IMEI Numbers in their respective import documents submitted to the KRA; all retailers and wholesalers of mobile devices ensure that they only retail or distribute mobile devices that are tax compliant and mobile network operators to only connect devices to their networks after verifying the tax compliance status through a whitelist database of compliant devices, provided by KRA. Operators were also required to provide for grey-listing non-compliant devices.

3. Following the above, on 5th November 2024, the 2nd respondent posted a public notice on its X account and website requiring all importers to submit detailed import entries that include accurate quantities, comprehensive model descriptions, and the respective IMEI numbers for each mobile device. Device assemblers and manufacturers to register on the KRA Customs Portal and submit a report of all devices assembled for the local market along with their respective IMEI numbers. Passengers entering Kenya were to declare their mobile devices on the F88 passenger declaration from, providing necessary details and IMEI numbers of the devices intended for use during their stay in the country.

Petitioner

4. The petitioner, a public interest litigant, filed this petition to challenge the notices as violative of the right to privacy, a fundamental freedom guaranteed in the Bill of Rights. The petition is supported by affidavits of Nora Mbagathi and Anand Venkatanarayanan.

5. The petition was brought against the Communications Authority of Kenya, KRA and The Attorney General as the 1st, 2nd and 3rd respondents respectively. Data Privacy and Governance Society Kenya; International Commission of Jurists (Kenya); Law Society of Kenya and The Consumers Federation of Kenya were joined as the 1st to 4th interested parties while Ideate Tech Policy Africa Limited was joined as amicus curiae.

6. The petitioner took issue with the new requirement that individuals declare IMEI numbers of their mobile devices. According to the petitioner, upon registration of mobile phones IMEI numbers constitute personal data and when read in connection with certain data held by mobile service providers, IMEI numbers can easily identify a person's sensitive personal information.

7. The petitioner asserted that the new practice of whitelisting devices means that only a device whose IMEI is registered on the CAK and KRA databases can connect to mobile networks thus, anyone who does not register IMEI number cannot buy a SIM-card from mobile network providers in Kenya. The petitioner again asserted that creation of a master database to give comprehensive access to personal IMEI numbers to government authorities threatens the right to privacy and is the first step towards possible mass surveillance.

8. The petitioner took the view, that whitelisting is unnecessary because there exists blacklist where information on stolen phones is shared and intended to achieve the same goal of ensuring that phones improperly in circulation can be identified. The petitioner averred that the notices have further ramifications on the realisation of the entire constitutional framework. When individuals know that they may be monitored, they may become more cautious about what they say, write or do which may lead to self-censorship, especially on political, religious or controversial topics.

9. The petitioner stated that the impugned notices violate the principle of separation of powers and usurp the mandate of Parliament in article 94 of *the Constitution* since the notices were not tabled in Parliament for scrutiny as required by the *Statutory Instruments Act*.

10. According to the petitioner, to the extent that the impugned notices require mandatory disclosure of IMEI numbers by individuals and importers, the right to privacy guaranteed under article 31 of *the Constitution* is threatened. The notices further violate the Data Protection Act on the premise that there is lack a genuine consent as required by regulation 4(3) and 4(4) of the Data Protection (General) Regulations, 2021 and failure to conduct a Data Impact Assessment as required by section 31 of the Data Protection Act and regulation 49 of the Regulations.

11. The petitioner asserts that the respondents' actions further violate articles 10, 24, 27, 28, 35(3) and 47 of *the Constitution* and that in coming up with the notice, CAK acted ultra vires its mandate. According to the petitioner, IMEI numbers are unique and are tied to a mobile device irrespective of whether they are classified as smart phones or not. IMEI number provides information about the phone, such as the brand, the year of production and some other technical specifications. IMEI numbers of devices owned by individuals fit the definition of personally identifiable information when combined with other information such as the person's name, SIM Card information, or phone number, hence the need for protection.

12. The petitioner stated regarding fraud and cybercrime, that a commonly shared IMEI blacklist is sufficient and there exist systems to identify and prevent circulation of stolen or improper phones on the Kenyan and international markets. A whitelist containing all IMEI numbers tied to individual's resident is excessive, unnecessary and a building block of a surveillance state.

13. It was asserted that mobile phone operators have information on which SIM card is tied to which IMEI. When the phone rings to the closest cell phone tower, the mobile company can locate the phone within a 100m radius depending on the tower density and technology used. If the government's whitelist IMEI database is linked to mobile phone operators they can access information directly without a warrant, by running simple queries.

14. It is the petitioner's view, that collection of IMEI information required by the impugned notices is excessive and the risks associated with collection; processing and storage of IMEI numbers override the legitimate aims of reducing revenue loss and combating fraud and cybercrime.

15. The petitioner sought the following relief:

    a. A declaration that the Impugned notices are unconstitutional, null and void for failure to comply with Articles 94 and 95 of *the Constitution* and *Statutory Instruments Act* Cap. 2A.

    b. An order of certiorari quashing the respondents' notices to collect, process and store IMEI Numbers in Kenya without undertaking and proactively publishing a Data Protection Impact Assessment contrary to Section 31 of the *Data Protection Act, 2019* Cap. 411C and *Access to Information Act* CAP 7M.

c. An order of mandamus compelling the respondents to conduct and/or make public a compliant Data Protection Impact Assessment.

d. A declaration that the establishment of a whitelist register is discriminatory and contrary to Article 27 of *the Constitution*.

e. A declaration that the regulation requiring individuals to disclose the IMEI numbers after registering their phones violates their right to privacy and is contrary to article 31 of *the Constitution*.

f. A declaration that the respondents' actions violate Articles 10, 19, 20, 21, 27, 28, 31 47, 94 and 95 of *the Constitution* of Kenya.

g. An order of prohibition prohibiting the respondents and any other state agency from implementing or acting upon the impugned notices.

h. Any other prayers this Court deems fit.

1st respondent's response

16. The 1st respondent opposed the petition through a preliminary objection; grounds of opposition and a replying affidavit sworn by Liston Cheruiyot Kirui.

Preliminary objection

17. In the preliminary objection, the 1st respondent contended that the jurisdiction of this court has been invoked wrongly and prematurely because the issues raised in the petition fall within the mandate of the Communications and Multimedia Appeals Tribunal established under the *Kenya Information and Communications Act* (Cap 411A). Other issues fall within the mandate of the Commission on Administrative Justice (CAJ). Additionally, the petition offends the provisions of section 9(4) of the *Fair Administrative Action Act*, 2015.

Grounds of opposition

18. The 1st respondent contended through the grounds of opposition that granting the relief sought would contravene the provisions of article 34 of *the Constitution* on its mandate; that the petition violates the doctrine of issue estoppel because the Court of Appeal in Communications Authority of Kenya v Okiya Omtatah Okoiti & Others [2020] KECA 754 (KLR) already determined the issues raised.

19. It is the 1st respondent's position that the petitioner has misunderstood the IMEI system. The IMEI number is a technical identifier for the device itself and does not disclose or track the personal identity of the user. Ownership changes of a mobile device do not affect the IMEI number hence it does not infringe on the right to privacy.

20. The 1st respondent stated that under Kenya Information and Communications (Registration of SIM cards) Regulations, 2015, Mobile Network Operators are required to maintain a database containing detailed personal information of all registered SIM card users. This information directly ties the SIM card to the individual, ensuring a verifiable connection between the users and their communications. In contrast, IMEI numbers are device specific technical identifiers that distinguish one mobile device from another. They are further used for managing network access, preventing theft and identifying and distinguishing devices but do not store or reveal information about the user thus, cannot be used for any form of surveillance.

21. The 1st respondent maintained that the alleged violations in relation to privacy fall within the jurisdiction of the Office of the Data Protection Commissioner.

Replying affidavit

22. In the replying affidavit, it was stated that the notice is collaborative in nature and is meant to compensate for lack of the 1st respondent's physical presence at the ports of entry. It therefore establishes a framework whereby the 2nd respondent's officials coordinate closely with their counterparts at the 1st respondent to facilitate thorough verification and physical processes of imported electronic devices.

23. The 1st respondent asserted that the notice requires importers to upload IMEI numbers of all devices to the 2nd respondent's approved portal. The 2nd respondent will then verify that the imported devices match those declared by the importer, thereby preventing tax evasion. At the same time, the 1st respondent will ensure that only devices conforming to a type-approved model are permitted, by checking and confirming that each device has a valid IMEI in accordance with the type approved model.

24. The 1st respondent contended that IMEI number is a globally standardized, 15-digit identifier assigned to mobile communication devices such as phones, tablets and data cards. Only devices that connect to GSM network possess an IMEI which identifies the mobile device by conveying details such as its identity, model, manufacturer, and a unique serial number assigned by the manufacturer. Consequently, every imported or locally manufactured mobile device comes with IMEI number.

25. The 1st respondent maintained that issuance and management of IMEI numbers is governed by the Global System for Mobile Communications Association and IMEI number uniquely identifies mobile devices and enables regulators, manufacturers, and service providers to address issues such as theft, counterfeiting and unauthorized network access.

26. The 1st respondent asserted that when a mobile device is switched on, it transmits its IMEI to the network even in the absence of a sim card. Without a sim card, IMEI number alone cannot be linked to personal information. Only mobile network operators can associate a sim card with a device's IMEI number

27. The 1st respondent maintained that IMEI is a technical identifier confined to the device itself. It is not linked to user behaviour or activities nor does it contain or collect personal data. Its role is to verify the authenticity or hardware and ensure that devices comply with established standards without enabling surveillance or user monitoring.

28. The 1st respondent asserted that the impugned notice requires that IMEI number be uploaded into a database at specific stages during local assembly, importation, or prior to sale by retailers or wholesalers-before they are sold to end users. At these stages, the IMEI can only be used to verify compliance with type approval standards, confirms that devices are neither counterfeit nor stolen, and ensure that customs duties have been collected. In this context, it does not pose any risk of violating privacy or enabling surveillance.

29. The 1st respondent stated that under the Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, any device used to connect to public networks must be type-approved by the authority. At points of entry, importers are required to provide evidence that the devices being imported had been type-approved by attaching a type-approval certificate to the import declaration form. In order to ensure that the devices being imported

conform to the declaration, such importers are now required by the impugned notice to key in the IMEI numbers of all mobile devices in that consignment.

30. The 1st respondent refuted the claim that the notice is a statutory Instrument so as to require compliance with the *Statutory Instruments Act*. The 1st respondent denied the petitioner's assertion that blacklists for stolen phones are sufficient. That argument disregards the GSM standard's deliberate three-tiered design which serves distinct and complementary regulatory purposes. The whitelist, grey list and blacklist all serve distinct roles to ensure that the integrity in the communication sector is maintained.

31. The 1st respondent contended that IMEI numbers do not constitute personal data as defined under section 2 of the Data Protection Act. The purpose, scope and context of collecting IMEI numbers do not pose any risks to the rights and freedoms of data subjects as the data remains anonymized and unrelated to personal information. The 1st respondent is therefore under no obligation to conduct a data protection impact assessment. The 1st respondent maintained that the petitioner's allegations on violation of article 35 of *the Constitution* is premature and there is also no basis for the argument regarding mass surveillance.

2nd respondent's response

32. The 2nd respondent opposed the petition through a replying affidavit (sworn by Peter Olali.) The 2nd respondent stated that it has authority under articles 209 and 210 of *the Constitution* to ensure it effectively assesses, collects and accounts for all tax revenues due under various tax laws. In order ensure that everybody pays their fair share of taxes and within reasonable recovery measures, *the Constitution*, the *Excise Duty Act* (Cap 472), the *Value Added Tax Act* (Cap 476), the *Miscellaneous Fees and Levies Act* (Cap 469C), the East African Community Customs Management Act (2004) and other relevant laws have provisions that enable it to demand tax, investigate tax evasions and ensure that tax due is paid by parties responsible.

33. The 2nd respondent asserted that it is dedicated to fostering tax compliance and enhancing revenue collection as part of its commitment to national development and in collaboration with the 1st respondent in regulating importation of mobile devices. The impugned notice is an initiative to ensures proper tax declaration, payment and verification of mobile devices imported into or assembled within Kenya.

34. The 2nd respondent contended that the impugned notice is aimed at enhancing revenue collection, promote fair tax practices, support national development, enhance transparency and reduce tax evasion. The 2nd respondent asserted that it has no powers or mechanisms to monitor or engage in any form of surveillance. The IMEI is a phone identifier and has nothing to do with tracking and surveillance. Its goal is to ensure that all mobile devices in use are legitimate and meet the necessary tax obligations and regulatory requirements.

35. Regarding violation of privacy, the 2nd respondent stated that all information and data received is for tax purposes and is solely handled in line with the provisions of *the Constitution*, the *Excise Duty Act*, the Value Added Tax, the East African Community Customs Management Act and the *Miscellaneous Fees and Levies Act*, among other relevant tax laws.

36. According to the 2nd respondent, the information sought regarding registration of IMEI does not violate the Data Protection Act. It is done at the point of importation by importers and assemblers and the details of the end user are not captured anywhere. In any event, the 2nd respondent asserts,

it is compliant with the requirements of the Data Protection Act and the General Data Protection Regulations.

37. The 2nd respondent maintained that data collected is limited to what is required to ensure compliance with applicable tax laws as and system access to data is role-based. Its data accountability framework holds staff accountable for proper data use. The 2nd respondent urged that the right to privacy under article 31 of *the Constitution* is not absolute. Further, provision of IMEI numbers meets the constitutional and statutory threshold. According to the 2nd respondent, sections 5(4), 9(2) and 191 of the East African Community Customs Management Act and section 6(1) of the *Tax Procedures Act* ensure protection of the citizen's personal information from disclosure.

38. The 2nd respondent denied the claim of discrimination against any citizen or violation of the right to dignity. The 2nd respondent asserted that information registered in its Customs Declaration System is general in nature and does not capture personal information. It has a duty under section 18(2) of the East African Community Customs Management Act, 2004 to ensure that all goods importation of which is for the time being regulated by the Act or by any written law and the conditions or guidelines for their importation are complied with.

3rd respondent's response

39. The 3rd respondent opposed the petition through grounds of opposition. The 3rd respondent asserted that IMEI registration framework is grounded on the statutory and constitutional mandate of the 1st and 2nd respondents as stipulated in the *Kenya Information and Communications Act* and *Kenya Revenue Authority Act*.

40. According to the 3rd respondent, IMEI registration framework resonates with the provisions of articles 201 and 209 of *the Constitution*. Collection of IMEI numbers is limited to a legitimate regulatory purpose and does not constitute arbitrary or unlawful interference with privacy; the right to privacy is not absolute and can be limited within the dictates of article 24. The framework aligns with the objectives of article 35 of *the Constitution* and the respondents issued public notices on the IMEI framework, ensuring stakeholder awareness and participation.

41. It was the 3rd respondent's position that articles 94 and 95 of *the Constitution* are wrongly invoked because the impugned notices are not legislative acts but administrative actions issued under the statutory mandate of the respondents. They did not require parliamentary approval under the *Statutory Instruments Act*.

42. The 3rd respondent asserted that the whitelisting mechanism is proportionate and non-discriminatory and that the dignity of individuals is not violated by registration of IMEI numbers. The 3rd respondent maintained that the relief to prohibit implementation of the notices is unwarranted as the measures being taken are integral to fulfilling Kenya's obligation under both domestic laws and international commitments to combat tax evasion, counterfeit goods and illicit trade.

43. The 3rd respondent stated that the Data Protection Act permits data processing where it is necessary and authorized for compliance with legal obligations or in the public interest under section 25(b). The 3rd respondent maintained that the framework adheres to *the Constitution* and statutory laws, striking a balance between individual rights and public interest.

44. The 3rd respondent took the view, that the existing blacklist system does not sufficiently address the challenges of counterfeit devices and tax evasion, and the whitelist system provides a more robust solution by proactively ensuring compliance before devices are connected to mobile networks. IMEI registration framework contributes to consumer protection in line with article 46 of *the Constitution*.

1st interested party's response

45. The 1st interested party supported the petition through a replying affidavit sworn by Mugambi Laibuta (Mr. Laibuta). It was stated an IMEI number is a unique identifier assigned to every mobile device with cellular capabilities; it creates the connection between a mobile phone device and a cell phone tower allowing mobile providers to pinpoint a phone's location within a defined radius; allows cellular networks to identify the device being used on their network, ensuring that each device is distinguishable; it can be used to locate a lost or stolen phone, or mobile phone device that has been used to commit a crime; it can be used to identify and prevent the sale or use of counterfeit devices and may be used verify mobile device ownership.

46. According to the 1st interested party, due to the uniqueness and use, an IMEI number raises privacy concerns, namely; it can be used for tracking a device's location through cellular networks which in effect could infringe on a user's right to privacy under article 31 of *the Constitution* and the Data Protection Act if conducted without consent or legal authorization. Mobile applications and third-party services can access it using them for analysis, targeted advertising or creating user profiles across devices.

47. The 1st interested party stated that when combined with other data points such as location, mobile application usage, phone number, flight and customer information, name, age, sex and other identifiable personal information, an IMEI number can contribute to user profiling, behavioural tracking and surveillance by state agents.

48. In the view of the 1st interested party, since an IMEI number can easily identify an individual, it is personal data within the definition in section 2 of the Data Protection Act. If databases containing IMEI numbers are compromised, they could be linked with personal data, leading to potential misuse.

49. The 1st interested party asserted that pursuant to section 25 of the Data Protection Act, the respondents ought to have valid legal basis for requiring disclosure and collection of IMEI numbers but have not shown the inefficiency of other methods of enforcing tax compliance. Using IMEI numbers to secure tax compliance is unjustified and leads to potential violation of fundamental rights and freedoms.

50. The 1st interested party maintained that submitting a buyer of a mobile device to surveillance for purposes of tax compliance amounts to shifting the burden of compliance to a purchaser who is not the taxpayer for purposes of tax compliance. The public was not also involved before the impugned notices were issued. According to the 1st interested party, the respondents are obligated to inform mobile phone device users on how their IMEI numbers will be used, stored and shared. The respondents further have not met their disclosure requirements under section 29 of the Data Protection Act.

51. The 1st interested party asserted that IMEI numbers should only be collected and used for specific, explicit and legitimate purposes which the respondents have not demonstrated. Being personal data, it should only be retained as long as necessary for the intended purpose, which period has not been indicated contrary to section 25 of the Data Protection Act. The respondents had also not provided proof of security of the IMEI data that they want disclosed; disclose all third parties that will have access to the IMEI data and how they will use the data and the safeguards they have put in place for processing or publishing a Data Protection Impact Assessment as required under section 31 of the Data Protection Act.

52. The 1st interested party maintained that handling of IMEI numbers could lead to a violation of the right to freedom of expression, movement and freedom from discrimination. Operational costs will be unbearable for small scale business owners and local assemblers as a result of an added administrative

layer due to tax compliance and registration of IMEI numbers at the port of entry. The investment in compliance systems by small-scale players and local assemblers would push them out of the market space and allow larger and more aggressive players to dominate the industry.

53. The 1st interested party asserted that the threat of blacklisting IMEI numbers or blocking non-registered devices may prevent users from accessing essential services, such as mobile banking, affecting the marginalized groups. It could also lead to undermining the progress of the country in areas such as digital inclusion, online education, access to internet powered phones and technological growth and advancements.

54. The 1st interested party posited that in the absence of a cogent legislative support under which the respondents anchored the impugned notices, there is likely to be a hurdle in implementation of the directive, which will have far reaching consequences to businesses and consumers.

4th interested party's case

55. The 4th interested party supported the petition through an affidavit sworn by Stephen Mutoro. The 1st interested party stated that disclosure and registration of mobile device IMEI numbers is an affront on the right to privacy and data protection; exposes individuals to the risk of unjustifiable access to their personal data and communication.

56. According to the 4th interested party, the disclosure requirements imposed do not meet the limitation test under article 24 of *the Constitution*. Through the imposed measures (notices) the respondents do not demonstrate elaborate mechanisms for oversight and monitoring to ensure that handling of personal data by KRA and mobile network operators is done in an accountable manner and safeguarded from exploitative use for other purposes other than the tax purpose.

57. The 4th interested party was of the view, that in seeking to adopt measures that might expose individual's data and communications to exploitative use, the respondents have not demonstrated adequate measures to safeguard against surveillance and unauthorized interceptions.

Amicus Brief

58. The amicus cited an article 'Analysing of Security Risks Associated with IMEIs and Unwiped Data of Disposed Mobile Handsets, Vol.3, Issue 11, International Research Journal of Modernization in Engineering Technology and Science', Raja Sharma and Krishan Kumar and Prabhpreet Kaur, 'Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number' on the meaning of an IMEI number.

59. The amicus submitted that IMEI number constitutes personal data as it is obtained and linked to an individual immediately an individual purchase a mobile device. The Amicus relied on comparative analysis considered from, Paragraph 1.3 (xix) of the Nigerian Data Protection Regulations, 2019 and Paragraphs 171 and 172 of the European Data Protection Board (EDPB) Guidelines on processing personal data in the context of connected vehicles and mobility related applications.

60. The amicus again relied on article 5(3) of the European Union Data Protection Directive, The Privacy Directive (2002/58/EC, as Revised by 2009/136/EC), Section 2 of the Data Protection Act and a Report prepared by European Union Directorate General Justice Department Working Party; article 29 Data Protection Working Party Opinion02/2013 on Apps on Smart Devices, 00461/13/EN-WP 202 on the guiding principles for storage, processing and access to personal data.

61. The amicus submitted that based on the foregoing characterization of IMEI, it follows that it ought to be processed in line with the provisions of articles 31 of *the Constitution* and sections 25, 26, 30 and 31

of the Data Protection Act. The requirement to disclose IMEI numbers poses a threat to violation of the right to privacy guaranteed under article 31 of *the Constitution* as read with various international laws and provisions of the Data Protection Act. Disclosure of IMEI number reveals the personal data of the data subjects which information exposes the data subject to tracking, monitoring and surveillance by third parties, including the respondents.

62. The Amicus relied on the decisions in Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR and Big Brother Watch and Others v United Kingdom APP. Nos. 58170/13, 62322/14 and 24960/15) and the handbook Kenya Revenue Authority, 'Tax Matters' Tax Evasion Edition, Issue 1. Amicus asserted that the respondents had not demonstrated that there are less restrictive means of achieving the desired objectives.

63. The amicus stated that should the court make a finding that the notices did not comply with constitutional and statutory requirements then it would be justified in quashing them. The Amicus cited section 107 of the *Evidence Act* and the Book, Constitutional Law, Doctrines and the Litigation of Fundamental Rights and Freedoms (Law Africa, Nairobi, 2023) to submit that in the present case, the respondents have sought to limit the right to privacy and urged the court to consider the test of limitation of fundamental rights and freedoms under article 24 of *the Constitution* and whether the limitation of the right to privacy passes the limitation test.

64. The amicus asserted that in exercise of their administrative powers, the respondents are under an obligation to comply with the provisions of articles 10 and 47 of *the Constitution* as read with the provisions of the *Fair Administrative Action Act*. The Amicus urged the court to consider the South African decision in State v Manamela & another CCT25/99 and grant the most appropriate relief.

Petitioner's rejoinder

65. The petitioner filed further affidavit (sworn by Nora Mbagathi.) in which it maintained that the concern with the proposed use and method of collection proposed by the respondent that means the IMEI number will constitute personal identifiable data. The petitioner reiterated that the 2nd respondent's notice requires all passengers to fill in the F88 passenger declaration form at the entry points together and disclose IMEI numbers of their phone devices. The form requires details of name of the passenger, passport number, date of arrival, flight number among others.

66. Although the petitioner agreed that IMEI numbers do not constitute personal data at the point of generation, the petitioner contended that in this case, the respondents intend to associate personally identifying information with the IMEI number at the customs level. The F88 form clarifies that it will contain personal information, linking the IMEI number to the person as a unique identifier.

67. The petitioner stated that the existing GSM whitelist described in the respondent's affidavit is different from the proposed IMEI device whitelist challenged in the petition. The existing whitelist relates to which devices are active on the mobile operator's network, whereas the whitelist challenged is unrelated concept that each individual device's IMEI number is registered by an authority other than a mobile operator and cross referenced with personal information of the device owner.

Petitioner's submissions

68. This petition was disposed of through written submissions with brief oral highlights.

69. The petitioner filed written submissions which Mr. Nyawa, learned counsel for the petitioner highlighted. Mr. Nyawa cited articles 94 and 94(5) of *the Constitution*; section 11 (3) and (4) of the *Statutory Instruments Act* and the decisions in Republic v Ministry of Health & 3 others Ex-parte

Kennedy Amdany Langat & 27 others [2018] eKLR; Kenya Country Bus Owners' Association & 8 others v Cabinet Secretary for Transport & Infrastructure & 5 others [2014] eKLR; George Ndemo Sagini v Attorney General & 3 others [2017] eKLR and SDV Transami Kenya Limited and 19 others v Attorney General & 2 others & another [2016] eKLR to reiterate that the impugned notice meet the definition of a statutory instrument and therefore should have been tabled in Parliament for scrutiny.

70. Learned counsel submitted that IMEI numbers constitute personal data and the requirement in the notices for mandatory disclosure of IMEI numbers by individuals violates the right to privacy under article 31 of *the Constitution*. The notices further violate article 31 in two ways, namely; lack of genuine consent and failure to conduct a data impact assessment. Counsel relied on section 31 of the Data Protection Act, articles 1 and 8 of the African Union Convention on Cyber Security and Personal Data Protection; regulations 4 (3),(4) and 49 of the Data Protection (General) Regulations and the decisions in Robinson, Julian v Attorney General of Jamaica [2019] JMCC Full 5; Mahdewoo v The State of Mauritius 2015 SCJ 177 and Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Exparte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party) [2021] KEHC 122 (KLR).

71. Mr. Nyawa again cited the decision in Seventh Day Adventist Church (East Africa) Limited v Minister for Education & 3 others [2017] eKLR; Muslims for Human Rights (MUHURI) & another v Inspector General of Police & 5 others [2015] eKLR and SDV Transami Kenya Limited and 19 others v Attorney General & 2 others & another [2016] eKLR for the argument that the limitation does not meet the requirements of article 24 of *the Constitution* because, no law grants the respondents the power to limit privacy rights as they purported to do in the impugned notices. The respondents did not expressly state the intention to limit the right to privacy or any other rights and the nature and extent of the limitation.

72. Learned counsel again relied on the decision in Hoffman v South African Airways 2000 (1) SA 1 (CC) and added that the impugned notices are not law and cannot be used to limit a constitutional right. Learned counsel reiterated that the notices do not meet the proportionality threshold required under article 24 of *the Constitution* and relied Robert K. Ayisi v Kenya Revenue Authority & Another [2018] KEHC 6948 (KLR). Mr. Nyawa argued that in a bid to fix revenue leakage, the respondents do not consider the risk that the measure poses to human rights such as economic freedom, right to dignity, equality and privacy.

73. Relying on article 35(3) of *the Constitution*, sections 3 (b), (d) and 5(1) (c) of the *Access to Information Act* and the decisions in Nairobi Law Monthly Company Limited v Kenya Electricity Generating Company & 2 others [2013] eKLR; Katiba Institute v Presidents Delivery Unit & 3 others [2017] eKLR and Brummer v Minister for Social Development and Others (CCT 25/09) [2009] ZACC 21 (at para 63) the counsel argued that the respondents were constitutionally required to proactively disclose information on the data protection impact assessment, information on where and how IMEI numbers will be stored and processed. Failure to publish information also violates articles 10(2) of *the Constitution*.

74. Mr. Nyawa cited article 10 of *the Constitution*, sections 5 and 13 of the *Statutory Instruments Act* and the decisions in Communications Commission of Kenya & 5 others v Royal Media Services Limited & 5 others [2014] eKLR; British American Tobacco Kenya, PLC formerly British American Tobacco Kenya Limited v Cabinet Secretary for Ministry of Health & 2 others; Kenya Tobacco Control Alliance & another (Interested parties); Mastermind Tobacco Kenya Limited (Affected Party) [2019] KESC 15 (KLR); George Ndemo Sagini v Attorney General & 3 others [2017] eKLR; Keroche Breweries Limited & 6 others v Attorney General & 10 others [2016] eKLR and Republic v Kombo & 3 others ex parte Waweru (2008) 3 KLR (EP) 478 to argue that the notices are unconstitutional for being

published without public participation. The notice by the 1st respondent is ultra vires because it goes beyond CAK's mandate and powers as it has no powers to pass regulations or policy guidelines on tax compliance.

75. Learned counsel argued that the impugned notices violate the right to fair administrative actions because they were issued without according the affected parties a hearing, beyond the statutory powers, without reasons and are unreasonable. counsel relied on article 47 of *the Constitution*, section 4(1) and 7 of the *Fair Administrative Action Act* and the decisions in Kenya Human Rights Commission & another v Non- Governmental Organizations Co-ordination Board & another [2018] eKLR; Republic v Fazul Mahamed & 3 others Ex-Parte Okiya Omtatah Okoiti [2018] eKLR and Kuto v Kenya Magistrates and Judges Association; Independent Electoral and Boundaries Commission & another (Interested Parties) [2023] KEHC 26157 (KLR).

76. Mr. Nyawa again relied on article 19 of *the Constitution* and the decision in Ahmed Issack Hassan v Auditor General [2015] KEHC 4712 (KLR) and Justice K.S. Puttaswamy (Retired). v Union of India and others (2017) 10 SCC 1 that the notices violate the right to human dignity.

77. Mr. Nyawa reiterated that the intended whitelisting in the impugned notices is discriminatory. because anyone who does not provide IMEI number cannot register with a mobile operator. The measure also creates a double standard whereby visitors are trusted not to violate their tax obligations when residents are not afforded the same trust. There is also indirect discriminate against the poor. He relied on article 27 of *the Constitution* and the decision in Gichuru v Package Insurance Brokers Ltd [2021] KESC 12 (KLR) and Fugicha v Methodist Church in Kenya (Suing Through its Registered Trustees) & 3 others [2016] KECA 273 (KLR).

78. Regarding jurisdiction of this court Mr. Nyawa argued that by virtue of article 165 (3) (b) (d) (i) and (ii) of *the Constitution*, this court has jurisdiction to hear and determine this petition. Counsel relied on the decision in Aukot & 2 others v National Security Council & 5 others; Law Society of Kenya (Interested Party) [2024] KEHC 336 (KLR) and William Odhiambo Ramogi & 3 others v Attorney General & 4 others; Muslims for Human Rights & 2 others (Interested Parties) [2020] eKLR.

79. According to Mr. Nyawa, the constitutional questions raised in the petition cannot be determined by Communications and Multimedia Appeals Tribunal, Commission on Administrative Justice or the Office of the Data Protection Commissioner. Counsel relied on NGOs Co-ordination Board v EG & 4 others; Katiba Institute (Amicus Curiae) [2023] KESC 17 (KLR); Nicholus v Attorney -General & 7 others; National Environmental Complaints Committee & 5 others (Interested Parties) [2023] KESC 113 (KLR); Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Ex Parte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party) (supra) and Gakenyis & 4 others v Cabinet Secretary Lands & 4 others [2024] KEHC 4573 (KLR).

1st respondent's submissions

80. Mr. Kipkogei, learned counsel for the 1st respondent submitted highlighting their written submissions that the petition offends the doctrine of exhaustion because the issues raised can be determined through alternative forums, namely; Communications and Multimedia Appeals Tribunal, Commission on Administrative Justice and Office of the Data Protection Commissioner. Counsel relied on the decisions in Wafula v Safaricom Limited & 4 others [2025] KEHC 229 (KLR); Tv Africa- Kenya Holding Limited v Communications Authority of Kenya [2023] KEHC 26848 (KLR); Speaker of the National Assembly v Karume [1992] KECA 42 (KLR); Albert Chaurembo Mumbo & 7 others v

Maurice Munyao & 148 others [2019] eKLR and Krystalline Salt Limited v Kenya Revenue Authority [2019] eKLR.

81. Learned counsel argued that the petition violates the doctrine of issue estoppel owing to the decision in Communication Authority of Kenya v Okiya Omtatah Okoiti & Others (supra). He relied on the decisions in Communications Commission of Kenya & 5 others v Royal Media Services Limited & 5 others [2014] KESC 53 (KLR).

82. Mr. Kipkogei maintained that the 1st respondent's notice is not a statutory instrument; is based on an existing legal framework and there was no requirement to comply with the *Statutory Instruments Act*. According to learned counsel, the notice is administrative in nature and relied on Republic v Attorney General; Law Society of Kenya (Interested Party); Ex-parte: Francis Andrew Moriasi [2019] KEHC 7013 (KLR.

83. Learned counsel argued that the 1st respondent has a collaborative approach with the 2nd respondent thus, the notice is justified, lawful and constitutional. According to learned counsel, the process serves a dual purpose: to safeguards consumers from substandard devices while ensuring compliance with tax obligations. The court should therefore not curtail this mandate. Counsel relied on the decision in Communications Authority of Kenya v Okiya Omtatah Okoiti & Others (Supra).

84. Mr. Kipkogei asserted the notice does not violate the right to privacy guaranteed under article 31 of *the Constitution* because IMEI numbers do not constitute personal data as defined under section 2 of the Data Protection Act and the time the local assembler is uploading IMEI numbers to the data base, the mobile device has not been sold to anyone and therefore there is no personal information. This is similar to importers, retailers and wholesalers when uploading IMEI numbers.

85. Learned counsel submitted that at this stage, IMEI numbers will only verify compliance with type approval standards, confirm that devices are neither counterfeit nor stolen and ensure that customs duties have been collected. Consequently, use of IMEI numbers in this context does not pose any risk of violating privacy or enabling surveillance, as its role remains strictly technical and regulatory. Counsel relied on the decision in Tumaz and Tumaz Enterprises Limited & 2 others v National Council for Law Reporting [2022] KEHC 14747 (KLR).

86. Mr. Kipkogei maintained that the notice does not violate the Data Protection Act and there was no need for a data impact assessment before being issued. According to counsel, the notice is not legislation and does not create new limitations beyond those established by the existing legislation which enjoys the presumption of constitutionality. Counsel relied on the decision in Law Society of Kenya v Attorney General & another [2019] KESC 16 (KLR).

87. Learned counsel argued that even if the notice was to be construed as a measure limiting rights under *the Constitution*, it would still satisfy the proportionality test under article 24. counsel maintained that the notice does not impose arbitrary restrictions, does not violate articles 27, 28 and 35(3) of *the Constitution* and section 5(1) (c) of the *Access to Information Act* and did not require public participation. The 1st respondent did not act ultravires its mandate. Counsel urged the court to dismiss the petition with costs.

2nd respondent's submissions

88. Mr. Muhoro, learned counsel for the 2nd respondent also highlighted their written submissions first, that the petition is res judicata because the issues raised were dealt with in Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others (supra). Additionally, the notices invited stakeholders to send views before the commencement date and any grievances were addressed before then.

89. Learned counsel argued that the infringements alleged in the petition are hypothetical and not real threats and ought not be entertained. Reliance was placed on Wanjiru Gikonyo & 2 others v National Assembly of Kenya & 4 others [2016] eKLR.

90. Regarding violation of privacy, Mr. Muhoro maintained that information and data received is for tax purposes and is handled in line with the provisions of *the Constitution*, *Excise Duty Act*, the *Value Added Tax Act*, *Income Tax Act*, East African Community Customs Management Act, *Tax Procedures Act* and other relevant tax laws.

91. Learned counsel asserted that the information sought regarding registration of IMEI numbers does not in any way infringe on the provisions of the Data Protection Act and is registered for tax purposes. Registration of IMEI numbers is at the point of importation by importers and manufacturers and details of the end users are not captured anywhere.

92. Mr. Muhoro argued that the right to privacy is not absolute and may be limited by a law as permitted by article 24 of *the Constitution*. Counsel cited the decision in Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR that provision of IMEI numbers to the 2nd respondent meets the constitutional and statutory threshold and does not infringe the article 31 of *the Constitution* as it does not fall under the qualification unnecessarily required or revealed.

93. Learned counsel again relied on sections 58 and 59(1) of the Tax Procedure Act and the decision in Samura Engineering Limited and 10 others v Kenya Revenue Authority [2012] eKLR for the proposition that the law provides a comprehensive framework for the protection of personal data during tax enforcement. Counsel maintained that there is no discrimination against any citizen. On dignity, counsel asserted that the 2nd respondent's customs system is general in nature and does not capture personal information. He urged the court to dismiss the petition with costs.

3rd respondent's submissions

94. Miss Robi, learned counsel for the n3rd respondent relied on their grounds of opposition and argued that no issues were raised or orders sought against the 3rd respondent. Learned counsel prayed that the petition be dismissed.

1st interested party's submissions

95. Mr. Mutua, learned counsel for the 1st interested party substantively reiterated the contents of their replying affidavit. Counsel relied on the decisions in Kenya Legal and Ethical Network on HIC & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others [2016] KEHC 8450 (KLR); Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] KEHC 7494 (KLR); Samura Engineering Limited & 10 others v Kenya Revenue Authority [2012] KEHC 5672 (KLR) and Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication ad Technology & 2 others; Katiba Institute another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party) (supra) on the critical nature of the right to privacy in Kenya and the need for data protection impact assessment.

96. Mr Mutua pointed to incidences where the Kenyan security agents have had access mobile phone users' information and location data held by telecommunications. Learned counsel submitted that the impugned notices are unconstitutional, for having not followed constitutional and legislative procedures before being published. He urged the court to allow the petition.

Determination

97. Upon considering the pleadings and arguments by parties, the issues for determination are whether this court has jurisdiction; whether the petition is res judicata and depending on the answer to these issues, whether the impugned notices violate the right to privacy.

Jurisdiction

98. The respondents argued that this court has no jurisdiction to determine this petition because there exist alternative dispute resolutions mechanisms the petitioner should have invoked before approaching this court, namely; Communications and Multimedia Appeals Tribunal; Commission on Administrative Justice (CAJ) and Office of the Data Protection Commissioner. The respondents relied on several decisions, including Wafula v Safaricom Limited & 4 others [2025] KEHC 229 (KLR); Tv Africa-Kenya Holding Limited v Communications Authority of Kenya [2023] KEHC 26848 (KLR); Albert Chaurembo Mumbo & 7 others v Maurice Munyao & 148 others [2019] eKLR and Krystalline Salt Limited v Kenya Revenue Authority [2019] eKLR.

99. The petitioner, supported by the 1st interested party maintained that this court has jurisdiction by virtue of article 165 (3) (b) (d) (i) and (ii) of *the Constitution* since the issue raised is on violation of rights and fundamental freedoms in the Bill of Rights. They relied on the decisions in Aukot & 2 others v National Security Council & 5 others; Law Society of Kenya (Interested Party) [2024] KEHC 336 (KLR) and William Odhiambo Ramogi & 3 others v Attorney General & 4 others; Muslims for Human Rights & 2 others (Interested Parties) [2020] eKLR.

100. Jurisdiction is the power or authority given to a court to hear and determine disputes before it. Challenge to jurisdiction is a threshold and fundamental question that the Court has to determine as soon as possible. If the Court finds that it has no jurisdiction to hear a matter, that is the end. The Court should not take any further step. It must down its tools. (See Owners of Motor Vessel "Lillian S" v Caltex Oil (Kenya) Limited [1989] KECA 48 (KLR)).

101. The question of a court's jurisdiction to hear a matter is to be determined based on the facts of the matter before it by carefully considering and determining the fundamental question of whether it has jurisdiction over that particular matter. Where the Court determines that it has no jurisdiction to hear the matter, it will have no power to proceed beyond that point.

102. Speaking on jurisdiction in Samuel Kamau Macharia v Kenya Commercial Bank Ltd & 2 others [2012] eKLR, the Supreme Court stated:

> (68) A Court's jurisdiction flows from either *the Constitution* or legislation or both. Thus, a Court of law can only exercise jurisdiction as conferred by *the constitution* or other written law. It cannot arrogate to itself jurisdiction exceeding that which is conferred upon it by law... without jurisdiction, the Court cannot entertain any proceedings...Where *the Constitution* exhaustively provides for the jurisdiction of a Court of law, the Court must operate within the constitutional limits. It cannot expand its jurisdiction through judicial craft or innovation.

103. In re the Matter of the Interim Independent Electoral Commission (Applicant), Constitutional Application Number 2 of 2011 [2011] eKLR, after referring to Owners of Motor Vessel "Lillian S" v Caltex Oil (Kenya) Limited (supra), the Supreme Court observed:

> (30) The Lillian 'S' case establishes that jurisdiction flows from the law, and the recipient-Court is to apply the same, with any limitations embodied therein. Such a Court may not arrogate to itself jurisdiction through the craft of interpretation, or by way of endeavours to discern

or interpret the intentions of Parliament, where the wording of legislation is clear and there is no ambiguity. In the case of the Supreme Court, Court of Appeal and High Court, their respective jurisdictions are donated by *the Constitution*.

104. It follows that jurisdiction of a court must flow from *the Constitution*, statute or both. The court should only exercise jurisdiction as conferred on it by *the Constitution* or the law. It must not act without jurisdiction or through innovative interpretation so as to confer jurisdiction on itself.

105. Section 6 of the *Fair Administrative Action Act*, 2015 provides that a person who is aggrieved by an administrative action or decision may apply for review of the administrative action or decision to a court in accordance with section 8; or a tribunal in exercise of its jurisdiction conferred in that regard under any written law.

106. Section 9(1) of the Act provides that subject to subsection (2), a person who is aggrieved by an administrative action may, without unreasonable delay, apply for judicial review of any administrative action to the High Court or to a subordinate court upon which original jurisdiction is conferred pursuant to article 22(3) of *the Constitution*. Subsection (2) states that the High Court or a subordinate court under subsection (1) should not review an administrative action or decision under the Act unless the mechanisms including internal mechanisms for appeal or review and all remedies available under any other written law are first exhausted.

107. Under subsection (3), The High Court or a subordinate Court should, if not satisfied that the remedies referred to in subsection (2) have been exhausted, direct the applicant to first exhaust such remedies before instituting proceedings under subsection (1). Sub section (4) states that notwithstanding subsection (3), the High Court or a subordinate Court may, in exceptional circumstances and on application, exempt such person from the obligation to exhaust any remedy if the court considers such exemption to be in the interest of justice.

108. The import of section 9(2) is that a person who is aggrieved by an administrative action may, without unreasonable delay, apply for judicial review of any administrative action to this Court or to a subordinate court upon which original jurisdiction is conferred pursuant to article 22(3) of *the Constitution* after being satisfied that alternative remedies have been exhausted. If not, the court should direct the person to first exhaust such remedies before instituting proceedings before it.

109. The petitioner' case is that the 1st and 2nd respondents' notices will violate the right to privacy and were issued without following the law. The Notices, the petitioner argued, threaten to violate a right guaranteed in the Bill of Rights and are therefore unconstitutional.

110. The respondents argued that this court has no jurisdiction because there is are alternative forums for resolving the dispute being the Communication of Kenay Act; The Data Protection Act and Commission on Administrative Justice, and therefore, section 9(2) of the *Fair Administrative Action Act* requires that the alternative remedy be exhausted before approaching the court.

111. Indeed, Communications and Multimedia Appeals Tribunal; Office of the Data Protection Commissioner and Commission on Administrative Justice have mandate to determine disputes falling within their respective jurisdictions, namely under the statutes establishing these institutions. However, these organs can only deal with matters that can adequately be determined by those administrative bodies. In other words, the administrative bodies must be capable of giving an effective or efficacious remedy. The person raising the jurisdictional question on account of availability of alternative remedy, must show that the administrative body not only has mandate to resolve the dispute(s) or issue(s) raised in the petition, but also that the remedy is effective.

112. The respondents did not argue that the remedies that the mentioned administrative bodies can give under the relevant laws are efficient and efficacious in the circumstances of the petitioner's case.

113. In Union of India v. T.R. Vermai, 1957 AIR 882, 1958 SCR 499, the Supreme Court of India stated that "when an alternative and equally efficacious remedy is open to a litigant, he should be required to pursue that remedy and not to invoke the special jurisdiction of the High Court to issue a prerogative writ."

The court was clear that the alternative remedy should be efficacious or effective.

114. In Albert Chaurembo Mumbo & 7 others v Maurice Munyao & 148 others [2019] KESC 83 (KLR), the Supreme Court stated (at para 116) that "where there exists an alternative method of dispute resolution established by legislation, the courts must exercise restraint in exercising their jurisdiction conferred by *the constitution* and must give deference to the dispute resolution bodies established by statute with the mandate to deal with such specific dispute in the first instance "

(See also Abidha Nicholus v Attorney General & 7 others; National Environmental Complaints Committee (NECC) & 5 others (Interested Parties) [2021] eKLR.)

The position to be drawn from the jurisprudence is that there should not only be an alternative remedy but the available remedy should be effective or efficacious for purposes of resolving the dispute.

115. This Court holds the view, that where the controversy is a question calling for resolution of a constitutional issue and especially whether a right and fundamental freedom in the Bill of Rights has been violated; infringed or is threatened; interpretation of *the Constitution* or both, such an issue can only be decided by this court instead of dismissing the petition on the ground of availability of an alternative remedy provided for by statute.

116. This view is informed by the fact that article 22 of *the Constitution* grants every person the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened. Article 23 (1) then confers on the Court jurisdiction as read with article 165, to hear and determine the application for redress of denial, violation or infringement of, or threat to, a right or fundamental freedom in the Bill of Rights or interpretation of *the Constitution* while article 23 (3) provides for the remedies the court may grant in respect of proceedings brought under article 22.

117. Under article 165(3) (b) this court has jurisdiction to determine the question whether a right and fundamental freedom in the Bill of rights has been denied, violated, infringed or is threatened. And indeed, section 9(1) of the *Fair Administrative Action Act* acknowledges that original jurisdiction is conferred on this court by *the Constitution*. In that regard, everything else, including exhaustion of available alternative remedy does not oust the court's jurisdiction but is subject to the nature of the claim brought before the court under *the Constitution*.

118. As the Supreme of India observed in Godrej sara lee Ltd v the Excise and Taxation Officer-Cum-Assessing Authority & Others (Civil Appeal No 5393 of 2010) (1st February 2023) "entertainability" and "maintainability" of a writ petition are distinct concepts. Availability of an alternative remedy does not operate as an absolute bar to the "maintainability" of a writ petition. The rule which requires a party to pursue the alternative remedy provided by a statute is a rule of policy, convenience and discretion rather than a rule of law.

119. In the circumstances of this petition, the respondents did not demonstrate that the alternative remedy available would be effective, taking into account the fact that the petition seeks declarations of invalidity of the impugned notices. This is because the jurisdiction of this Court is donated by *the Constitution*

and my reading of article 165(3) (b) on this court's jurisdiction is to, among others, determine the question whether a right or fundamental freedom in the Bill of Rights has been denied, violated, infringed or threatened; (d) (ii) the question whether anything said to be done under the authority of this Constitution or of any law is inconsistent with, or in contravention of, this Constitution.

120. Article 165(3) thus, confers on this court unlimited jurisdiction in criminal and civil matters except as limited by clause (5) regarding those matters reserved for other courts by article 162 (2) and restricted by clause (6). In that regard, the sweep of the constitutional authorisation given to this court should be viewed through the prism of article 165(3). Any claim that this court has no jurisdiction except as highlighted above does not find favour with article 165(3). This court can only decline to exercise jurisdiction so that parties can approach available alternative statutory remedies where the remedy is efficacious, but not for want of jurisdiction.

121. The petitioner having brought this petition claiming violation of *the Constitution* and a threat to violate rights and fundamental freedoms in the Bill of Rights, the respondents' argument that the petitioner could have invoked available alternative dispute resolution mechanisms cannot succeed. That is, the petition questions a threat to violate *the Constitution* and rights and fundamental freedoms that may be occasioned by the impugned notices. I therefore find and hold that the issues raised in this petition fall within the jurisdiction of this court.

Res judicata

122. The respondents again argued that the petition is res judicata because the issue raised was dealt with in Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others (supra), a fact the petitioner and the 1st interested party denied.

123. Section 7 of the *Civil Procedure Act* provides that "No court shall try any suit or issue in which the matter directly in issue has been directly and substantially in issue in a former suit between the same parties, or between parties under whom they or any of them claim, litigating under the same title, in a court competent to try such subsequent suit or issue in which such issue has been subsequently raised, and has been heard and finally determined by such court."

124. Res judicata is a bar to further litigation on issues that have been previously litigated upon between the same parties in a court of competent jurisdiction and the court has determined the issue with finality. The doctrine of res judicata protects finality in litigation over similar issues between the same parties in courts of competent jurisdiction and prevents re litigation of similar issues

125. In Kenya Commercial Bank Limited v Muiri Coffee Estate Limited & another (Motion No 42 of 2014) [2016] eKLR, the Court of Appeal had the following to say with regard to the essence of res judicata:

> Res judicata is a doctrine of substantive law, its essence being that once the legal rights of parties have been judicially determined, such edict stands as a conclusive statement as to those rights....[T]he doctrine of res judicata is to apply in respect of matters of all categories, including issues of constitutional rights.

126. The Supreme Court of Kenya also delt with the issue of res judicata in John Florence Maritime Services Limited & another v Cabinet Secretary Transport & Infrastructure & 3 others (Petition 17 of 2015) [2021] KESC 39 (KLR), stating:

> (58) Whenever the issue of res judicata is raised, the court will look at the decision claimed to have settled the issue in question; the entire pleadings and record of that previous case and the instant case to ascertain the issues determined in the previous case, and whether these are the

same issues in the subsequent case. The court should ascertain whether the parties are the same, or are litigating under the same title, and whether the previous case was determined by a court of competent jurisdiction.

127. The position in law is that for the plea of res judicata to succeed, the issues in the previous suit and the new suit should be similar; parties in the two cases be the same or litigating under the same title and issues in the former suit should have been finally determined by a court of competent jurisdiction. In making that determination, the court dealing with the plea of res judicata, should look at the pleadings and prayers sought in the two suits; the parties named in the former suit and the subsequent suit and the decision of the court in the previous suit to ascertain whether the matter was before a court of competent jurisdiction and the issues were indeed, similar and had been determined with finality.

128. To prove the plea of res judicata in the present petition, the respondents were required to adduce evidence to demonstrate that the issues in this petition had been determined with finality in the previous matter. However, the respondents merely made reference to the decision in Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others [2020] KECA 754 (KLR) arguing that the issues in this petition were determined in that appeal thus, this petition is res judicata. Even though the respondents made reference to that decision, they did not point out which paragraph dealt with the issues that are in this petition to enable the court determine whether indeed, this petition is res judicata.

129. Although the case referred to was against Communications Authority of Kenya, Networks Limited Cabinet Secretary, Information and Technology and The Attorney General, only Communication Authority of Kenya and The Attorney General are parties in this petition. The respondents did not show that the issue of constitutional invalidity of the impugned notices was at the core of that petition as is the case here.

130. I have perused the judgment in Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR which gave rise to the appeal and judgment in Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others [2020] KECA 754 (KLR). The petition delt with the government's plan to instal Device Management System (DMS) on mobile phone networks operating in Kenya for fear that the device would be used for surveillance of the population by eavesdropping on peoples' private communications in violation of the right to privacy.

131. It was the respondents' duty to show that the previous petition called on the court to determine the foundational issue of the constitutionality of the requirement to upload IMEI numbers on the KRA's portal and visitors to provide IMEI numbers of their phone devices at the point of their entry into Kenya. however as shown above, the decision in case referred to delt with a different issue from that in the present petition. The petitioner was also different although two of the respondents are the same as in this petition. In the premise, the test for res judicata was not met thus, the objection that this petition is res judicata fails.

Notices and Privacy

132. The petitioner, supported by the 1st interested party, argued that the impugned notices are a threat to the right to privacy guaranteed in the Bill of Rights and therefore are unconstitutional. The respondents maintained that the notices are lawful and constitutional. In the respondents' view, the notices do not violate the right to privacy.

133. There are two impugned notices issued by the 1st and 2nd respondents respectively. The 1st respondent issued a notice published on its website and X account giving the following directions that were to take effect from 1st January 2025:

1. All local assemblers must upload the International Mobile Equipment Identity (IMEI) Number of each assembled device to the KRA-provided portal to ensure that locally assembled devices are tax compliant.

2. All mobile phone importers (sale, testing, research or any other purpose) will be required to disclose the International Mobile Equipment Identity Number in their respective import documents submitted to the KRA. This disclosure is mandatory for the registration of the devices in the National Master database on Tax -compliant Devices.

3. Retailers and wholesalers of mobile devices must ensure that they only retail or distribute mobile devices that are tax compliant. The authority will provide the means by which the tax compliant status of mobile device can be verified before purchase by retailers or end-users.

4. Mobile network operators must ensure that they only connect devices to their networks after verifying the tax compliance status through a whitelist database of compliant devices which will be provided by the Authority. Operators will also be required to provide for grey-listing of non-compliant devices to facilitating regularization within a prescribed period, failure to which the devices will thereafter be blacklisted.

   These requirements were to apply to all devices imported or assembled in the country from November 1st 2024. All existing devices that will be on the Mobile Networks by 31st October 2024 would not be affected.

134. Following this notice, the 2nd respondent issued its own notice again published on its website and X account titled: "Declaration of Mobile Devices Incorporating IMEI Numbers at Importation" The 2nd respondent cited Part B of the Second Schedule to the East African Community Customs Management Act, 2004 on restricted imports on the basis that mobile devices require regulatory permits from the 1st respondent. The 2nd respondent pointed out that following the 1st respondent's public notice on enhancing integrity and tax compliance of mobile devices, the 2nd respondent was notifying that all importers of mobile devices and travellers would be required to submit detailed import entries for all mobile devices with accurate quantities, proper model descriptions/specifications and their respective IMEI numbers in the Customs system. Passengers entering the territory of Kenya would declare the details and respective IMEI numbers of their mobile devices intended for use during their stay in Kenya at the port of entry on the F88 passenger declaration form. Device assemblers/ manufacturers must register on the Custom portal and submit a report of all devices assembled for local market and their respective IMEI numbers.

135. The 2nd respondent's notice stated that one must obtain necessary regulatory clearances and permits from the 1st respondent. The 2nd respondent further stated that the public was therefore being notified of this requirement, which would be implemented effective 1st January 2025. "Specific guidelines on the system process and how to capture the devices and IMEI numbers for different users will be shared in due course." the notice concluded.

136. The petitioner argued that the notices have the potential to violate the right to privacy since an IMEI number is an identifier of a mobile device and once the device is purchased and connected to a network, it becomes personal data and can be traced to a particular person and therefore violates the right to privacy. The petitioner's argument was supported by the 1st interested party.

137. The respondents on their part argued that IMEI number being a unique identifier for a particular mobile device does not constitute personal data. In any case, they argued, the information is only

required before the mobile device is purchased and is not data as defined under the Data Protection Act.

138. From the contestation above, the question here is whether IMEI numbers are data to qualify for protection as privacy rights.

139. Section 2 of the Data protection Act defines data to mean information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

(d) where it does not fall under paragraphs *(a)*, (b) or *(c)*, forms part of an accessible record; or

(e) is recorded information which is held by a public entity and does not fall within any of paragraphs *(a)* to *(d)*.

140. From the above definition, IMEI number is information that qualifies under (a)(b) and (c). In the present circumstances, IMEI numbers are to be recorded as part of a relevant filing system and as recorded information, they will be held by a public entity and will be kept in a portal accessible by the public.

141. Article 4 (1) of the European Union General Data Protection Regulation (EU GDPR) defines 'personal data' to mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

142. Based on the definition of data both under the Data Protection Act and EU GDPR, the question here is whether IMEI number can be said to be personal data capable of protection under article 31 of *the Constitution*.

143. The petitioner argued that although IMEI numbers do not explicitly reveal the identity of an individual, their linkage to a device usage, positions, as well as the ability to access certain types of data means that it falls within the ambit of personal data.

144. The respondents indeed, admitted that IMEI numbers are unique identifiers for each mobile device. However, they took the view, that IMEI numbers do not constitute personal data. According to the respondents, at the time local assemblers and importers upload IMEI numbers onto the KRA data base, the mobile devices have not been sold to anyone and therefore do not contain personal information. They argued that the same position applies to retailers and wholesalers when uploading IMEI numbers onto the portal. It was the respondent's position that IMEI numbers will at this stage only verify compliance with type approval standards; confirm that the devices are not counterfeit or stolen and ensure that customs duties have been collected. Use of IMEI numbers in this context does not pose the risk of violating privacy or enabling surveillance since its role remains strictly technical and regulatory: They argued.

145. There can be no doubt that an IMEI number is the device's digital fingerprint. In that regard, once a mobile device with an IMEI number, the device's digital fingerprint is paired with a sim card and registered with a mobile network, it is capable of accessing personal details, such as the phone number

being used; the type of device; the location where the device is being used, calls made to and from the sim card inserted and used in the mobile device or hardware, among other details .

146. The IMEI number being the digital fingerprint of the device, becomes personal data as soon as it is associated with a person. This happens when one purchases a mobile device and activates it at which point it would often provide personal details such as name, email address, password or biometrics, should a person opt for face ID or finger print biometrics for unlocking the device. The IMEI number becomes personal data since at that point it is linked to other information belonging to the owner or user of the mobile device.

147. The respondents did not deny the fact that when a mobile device is purchased and registered with a mobile network the IMEI number is capable of disclosing other valuable data of the person using the device thereby requiring protection. This is so, because personal data refers to information relating to an "identified" or "identifiable" person from direct or indirect inference where various data points are capable of identifying that person.

148. In view of the fact that once IMEI number is linked with a mobile device and registered with mobile network is capable of linking with the mobile user's personal data, it is personal data thus, requires protection under article 31 of *the Constitution*. The article provides that every person has the right to privacy, including the right not to have information relating to his family or private affairs unnecessarily required or revealed and the privacy of his or their communications infringed. The right to privacy is guaranteed in the Bill of Right and should not be infringed without justifiable cause.

149. The respondents maintained that the right to privacy is not absolute and can be limited in terms of article 24 of *the Constitution*. They maintained that the impugned notices fit the requirements in article 24.

150. Article 24 provides that 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 and

    (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.

151. A provision limiting a right or fundamental freedom should 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. The limitation should not affect the right or fundamental freedom to the extent of derogating from the core or essential content of that right. The State or person seeking to justify a limitation has to demonstrate that the requirements of article 24 have been satisfied.

152. Article 24 calls for a two-stage approach in which a broad rather than a narrow interpretation is given to the fundamental rights enshrined in the Bill of Rights. That is; limitation has to be justified in that the right in the Bill of Rights is to be limited only by a law and to the extent only that the limitation is justifiable in an open and democratic society and does not negate the core or the essential content

of the right that is protected by Constitution. The respondents bore the duty to demonstrate that the limitation was by a law; that the limitation was justifiable in our open and democratic society and that there is no lesser restrictive measure.

153. The 1st respondent's notice did not make reference to any provision of law upon which it was issued bearing in mind that the 1st respondent is not a collector of customs and duties, to enable this court consider whether the provision of law passes the limitation test in article 24.

154. Similarly, the 2nd respondent's notice issued following that of the 1st respondent, made general reference to Pat B of the Second Schedule to the East African Community Customs Management Act on restricted imports. Part B has a list of restricted goods and, what is relevant here is item (1) which states that "All goods the importation of which is for the time being regulated under this Act or by any written law by the time being in force in the Partner State."

155. It is worth noting that the 2nd respondent's notice stated that "Specific guidelines on the system process and how to capture the devices and IMEI numbers for different users will be shared in due course." This was an admission that there were no rules, regulations, guidelines or other relevant and known mechanisms for processing the data (IMEI numbers) to be captured from the devices.

156. The *Statutory instruments Act* defines an instrument to mean any rule, order, regulation, direction, form, tariff of costs or fees, letters patent, commission, warrant, proclamation, by-law, resolution, "guideline" or other statutory instrument issued, made or established in the execution of a power conferred by or under an Act of Parliament under which that statutory instrument or subsidiary legislation is expressly authorized to be issued.

157. In the absence of "guidelines" there was no way the court would determine whether the guidelines meet the requirements of a law as an instrument for purposes of collecting and processing IMEI numbers as data. The respondents did not also explain what will happen to IMEI numbers once mobile devices associated with particular IMEI numbers are sold or purchased; paired with sim cards and registered with or connected to mobile networks, leaving not only danger but also real possibility of unlawfully accessing peoples' personal data, a right to privacy that is protected as a fundamental right

158. In Botha v Smuts and Another [2024] ZACC 22, the Constitutional Court of South Africa stated that privacy is an individual condition of life characterised by seclusion from the public, publicity and public scrutiny. The court further stated:

> (86) The right to privacy accordingly recognises that we all have a right to a sphere of private intimacy and autonomy without interference from the outside community. The right to privacy represents the arena into which society is not entitled to intrude. It includes the right of the individual to make autonomous decisions, particularly in respect of controversial topics. (underlining)

159. In R v Bykovels, 2024 SCC 6, the Supreme Court of Canada also stated that people have a reasonable expectation of privacy in today's overwhelmingly digital world.

160. In Justice K.S Puttaswamy (Rtd) v Union of India AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, the Supreme Court of India held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty."

161. Chandrachud J, observed that the right to privacy imposes on the State a duty to protect the privacy of an individual, corresponding to the liability that is to be incurred by the state for intruding the right to life and personal liberty. No civilized state can contemplate an encroachment upon them without the authority of law. "Privacy recognises the ability of individuals to control vital aspects of their lives

and safeguards the autonomy exercised by them in decisions of personal intimacies, matters of home and marriage, the sanctity of family life and sexual orientation, all of which are at the core of privacy."

162. The Court again stated:

> (64) A fundamental feature of *the Constitution* is the sovereignty of the people with limited Government authority. *The Constitution* limits governmental authority in various ways, amongst them Fundamental Rights, the distribution of powers amongst organs of the State and the ultimate check by way of judicial review.

163. Applying the above principles in the circumstances of this petition, the right to privacy being a fundamental right, if the respondents had their way and took control of IMEI numbers of mobile devices in the country, the State would most likely completely dominate the citizens and alter the relationship between citizens and the State so that no person can conduct routine activities through a mobile phone without the State knowing about his activities.

164. It is therefore the finding of this court and I so hold, that to the extent that the respondents' intention is to take control of IMEI numbers of mobile devices, pool them in a portal and control the numbers even after the devices paired with IMEI numbers have been purchased and registered with a network, the notices are a threat to the right to privacy and therefore violate *the Constitution* and the Data Protection Act.

Conclusion

165. Having considered the pleadings, arguments by parties, *the Constitution* and the law, the conclusion I come to, is that the petitioner has demonstrated that the respondents' notices are not based on any provisions of the law and threaten to violate articles 24 and 31 of *the Constitution* and the right to privacy. The respondents did not demonstrate that there is a lawful mechanism for processing IMEI numbers which once associated with mobile devices and registered with a mobile network, qualify as personal data protected under the Bill of Rights.

166. Consequently, and for the above reasons, the court makes the following declarations and orders it considers appropriate:

1. A declaration is hereby issued that the notices issued by the 1st and 2nd respondents are unconstitutional and unlawful and therefore null and void.

2. A declaration is hereby issued that the requirement that individuals disclose IMEI numbers after registering their phones violates their right to privacy contrary to article 31 of *the Constitution*.

3. An order of certiorari is hereby issued quashing the 1st and 2nd respondents' notices to collect, process and store IMEI numbers of mobile devices in Kenya.

4. An order of prohibition is hereby issued prohibiting the 1st and 2nd respondents and any other State agency from implementing or acting upon the notices issued by the 1st and 2nd respondents.

5. This being a public interest litigation, each party shall bear their own costs.

DATED AND DELIVERED AT NAIROBI THIS 18TH DAY OF JULY 2025

E C MWITA

JUDGE