Case Number:	Civil Appeal 166 of 2018
Date Delivered:	24 Apr 2020
Case Class:	Civil
Court:	Court of Appeal at Nairobi
Case Action:	Judgment
Judge:	Martha Karambu Koome, Daniel Kiio Musinga, William Ouko
Citation:	Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others [2020] eKLR
Advocates:	-
Case Summary:	**The petition which challenged an on-going process for the design and installation of a Mobile Management System (DMS) in the mobile communications sector was filed prematurely.** **Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others** **Civil Appeal No 166 of 2018** **Court of Appeal at Nairobi** **W Ouko (P), MK Koome, DK Musinga, JJA** **April 24, 2020** **Reported by Beryl Ikamari** ***Civil Practice and Procedure*** *- institution of a suit - ripeness - where a petition was brought to challenge an on-going process for the design and*

installation of a DMS in the mobile communications sector, on grounds that it threatened privacy rights - whether the suit was premature and hypothetical given that the design and functioning of the DMS was still under discussion.

***Constitutional Law** - national values and principles of governance - public participation - adequacy of public participation - where public participation and consultations, on the design and installation of a DMS in the mobile communications sector, were still on-going - whether it was possible at that stage to determine whether public participation for the DMS was adequate.*

***Constitutional Law**- fundamental rights and freedoms - consumer protection rights and rights to privacy - allegations that the proposed design and installation of the DMS by the Communications Authority of Kenya would give access to mobile communication device user's private information to third parties - whether under the circumstances consumer protection rights and rights to privacy were violated.*

***Constitutional Law** - constitutional petition - precision in drafting a constitutional petition - whether a petition disclosed any violations of consumer's rights to privacy.*

Brief facts

At the High Court, the petitioner challenged the proposed installation of a device known as the Mobile Management System (DMS) by the Communications Authority of Kenya (CAK). He said that it would occasion the infringement of various rights including rights to privacy, fair administrative action, property and consumer protection. The appellant explained that it was concerned about theft of mobile devices and the proliferation of counterfeit or illegal devices. It had therefore found it necessary to create a centralized Equipment Identification Register (EIR) which was the DMS. The creation of such a register was within its mandate. It was necessary

to facilitate the implementation of the DMS and creation of a system that could define and identify counterfeit devices and substandard goods, reported lost or stolen devices and instances of SIM boxing operations that had infiltrated the industry and were evading payment of licences and taxes.

In responding to the question of infringement of privacy rights, the appellant said that the system would not create automatic access to the call data records (CDR) or content of such calls concerning any mobile number and the access that was requested from the mobile operators EIR's and home location register was for purposes of identifying the IMEI, IMSI and MSISDN for each device. The respondent added that the DMS was at design stage and therefore the petition was premature and based on unfounded allegations.

The petition was successful. The High Court issued various orders including orders to the effect that the setting up of the DMS was unconstitutional as it was done without adequate public participation and was a threat to the privacy rights of mobile communication device users. The appellant was prohibited from setting up the DMS in that manner.

The appellant challenged the High Court's decision. It stated *inter alia* that the High Court failed to hold that the petition was premature or hypothetical and that it considered extraneous and unpleaded matters in concluding that the DMS threatened rights to privacy.

Issues

1. Whether a suit intended to challenge the proposed design and installation of the Mobile Management System (DMS) by the Communications Authority of Kenya was hypothetical and premature.
2. Whether there was adequate public participation in the proposed design and installation of the DMS.
3. Whether the installation of the DMS threatened the consumer's rights to

privacy.
4. Whether the pleadings as drawn disclosed any violations of consumer rights to privacy.

Held

1. As the first appellate court, the court had a duty to re-evaluate and re-analyse all the material that formed part of the pleadings and affidavit evidence which informed the decision of the High Court.
2. The case as pleaded in the petition filed by the 1st respondent was slovenly drawn; it was made up of generalized allegations that were wholly predicated on unsubstantiated statements taken from newspaper reports and statements made by unnamed technical experts. The probative weight to be given to statements of facts contained in newspaper cuttings, required the maker of the statement to appear in court and be subjected to court room processes for that statement to be admissible in evidence.
3. The pleadings were not elegantly drawn. In an adversarial system, a party was bound by their pleadings and that protected the other party from being ambushed with new claims in the course of a hearing.
4. A petition should set out with a reasonable degree of precision particulars about how alleged acts amounted to infringement of the person's constitutional rights. The petition and the supporting affidavits were based on allegations of what was feared could happen, conjectures or at best unconfirmed sources of information.
5. The High Court did not rely on the 1st respondent's pleadings alone. There was a supporting affidavit made on behalf of the 7th respondent which was responded to extensively. Considering that the overarching principle in the administration of justice was to do substantive justice, it was prudent to consider and determine all issues raised in the appeal.
6. The supporting affidavit of the 7th

respondent was in support of the petition and it had letters annexed to it. It was those letters that formed the foundation of the petition and not the unsupported allegations in the petition.

7. The High Court overlooked the statutory mandate of the appellant which was as stated in the Kenya Information and Communication Act, No 2 of 2018 (KICA) that was *inter alia* to licence and regulate postal information and communication services. The High Court also did not identify the actual probable evidence that led to the conclusion that DMS would intrude on privacy and even if there were issues of concern which were still being addressed. Another key concern that the High Court overlooked was the undisputed fact that there were acknowledged challenges in the sector which needed to be fixed.
8. In fixing challenges in the mobile communications industry, there was a strategy which was implemented in the 1st phase where about 1.8 million stolen and counterfeit devices were netted and switched off. However, the challenges escalated to another level where the purveyors of counterfeit devices became more high-tech and started cloning genuine IMEI numbers to the counterfeit devices whose detection was not possible. In addition, the appellant was also faced with proliferation of SIM boxing operators who were operating illegally without a licence or remittance of taxes in contravention of the law. Had the High Court considered the nature of those challenges, it would have arrived at a different conclusion. The High Court, in considering those challenges, would have balanced the right to privacy and allow the appellant execute its mandate while following the law and in consultation with the other players in the industry.
9. The High Court over concentrated on the interpretation of an aspect of the term ‘access’ in a narrow sense in regard to retrieving data which it took to mean intrusion of privacy of communication. The

High Court did not consider other aspects of ‘access’ such as making use of the resources to address the challenges at hand. In accessing the data there was fear that the right to privacy was likely to be infringed and that fear seemed to have preoccupied the High Court. The right to privacy was important but the issues of abuse by unscrupulous mobile operators also needed to be tackled so as to strike a balance between securing the right to privacy and dealing with the problem without infringing the right to privacy.

10. In setting out the DMS, in pursuit of the appellant’s mandate to regulate the mobile communication sector, the appellant had a duty to abide by the law. There was no concrete evidence that the DMS was going to spy or intrude on private communication other than the unsupported newspaper cuttings.
11. Courts could not undertake the appellant's mandate; they could only adjudicate concrete disputes. There was apprehension that rights could be infringed but it had not crystalized, as meetings with technical teams to discuss the design, architecture and configuration of the DMS were ongoing.
12. There was no credible evidence to demonstrate that the DMS was meant to spy on consumers’ private information other than to net out the illegal operators.
13. There was ongoing public participation. There were ongoing consultations on how the DMS would operate. Since that process was not completed, it would be premature to decide whether public participation was adequate or not, noting that there was no known science of determining that and such a determination would be based on a consideration of several factors.

Appeal allowed.

Orders:-

1. *The orders of the High Court of April 19, 2018 were set aside.*

	2. *In exercise of its mandate of developing a DMS system, the appellant had to continue with the consultations that were ongoing with the stakeholders and MNOs prior to the filing of the petition so as to complete the technical and consumer guidelines on the DMS.* 3. *The guidelines/ regulations should be subjected to public participation.* 4. *Each party to bear its costs of the appeal.*
Court Division:	Civil
History Magistrates:	-
County:	Nairobi
Docket Number:	-
History Docket Number:	HC Petition No. 53 of 2017
Case Outcome:	Appeal allowed
History County:	Nairobi
Representation By Advocates:	-
Advocates For:	-
Advocates Against:	-
Sum Awarded:	-

IN THE COURT OF APPEAL

AT NAIROBI

(CORAM: OUKO, (P), KOOME & MUSINGA, JJ.A)

CIVIL APPEAL NO. 166 OF 2018

BETWEEN

COMMUNICATIONS AUTHORITY OF KENYA.....APPELLANT

AND

OKIYA OMTATA OKOITI.....1ST RESPONDENT

BROADBAND COMMUNICATIONS

NETWORK LIMITED.....2ND RESPONDENT

CARBINET SECRETARY,

INFORMATION AND TECHNOLOGY.....3RD RESPONDENT

HON. ATTORNEY GENERAL.....4TH RESPONDENT

ORANGE –TELKOM KENYA.....5TH RESPONDENT

AIRTELL NETWORKS KENYA LTD.....6TH RESPONDENT

SAFARICOM LIMITED.....7TH RESPONDENT

COALITION FOR REFORMS AND

DEMOCRACY.....8TH RESPONDENT

ARTICLE 19 EAST AFRICA.....9TH RESPONDENT

(Being an Appeal from the judgment of High Court of Kenya

at Nairobi (Mativo, J.) dated 19th April, 2018

CONSOLIDATED WITH

CIVIL APPEAL NO 167 OF 2018

in

HC Petition No. 53 of 2017)

****

JUDGMENT OF THE COURT

[1] During the hearing, this appeal was consolidated with **Civil Appeal No 167 of 2018** for purposes of hearing and determination as they both arise from the same judgment. The key issues before us for determination are; whether the proposed installation of the device called Mobile Management System (DMS) by the Communications Authority of Kenya (CAK) hereinafter referred variously also as the appellant would herald an error of public control and eavesdropping of peoples' privacy by intercepting and recording of communication and mobile data; whether the appellant adequately engaged stakeholders or allowed public participation in the design and implementation of DMS; whether the dispute was taken to court prematurely, therefore an hypothetical question and whether the Judge misapprehended the mandate of the appellant.

[2] What triggered the dispute in this appeal was a series of letters by the appellant to the major stakeholders including the mobile network operators, (MNOs) who included the 5th, 6th and 7th respondents (who are the key mobile network providers). The letters generally requested the MNOs to provide access to the appellant's technical team for purposes of survey and installation of the said DMS. The factual background of the need to create the DMS system has a long and technical history which was narrated in the affidavits of ***Francis Wangusi*** the then Director General of the appellant that were sworn on 21st March, 2017 and 5th October, 2017 respectively.

[3] These facts do not seem to have been controverted by any of the respondents, even after the 7th respondent was granted leave to file a further affidavit none was filed. The summation of the relevant facts are as follows; the regulation of the mobile communication since its advent in Kenya in early 2000, was guided by the world-wide global system for mobile communication (GSM). This process is regulated by various international agreements where it was agreed that in order to identify mobile communication devices that have been manufactured with regard to GSM standard, the said device had to bear identification mark of quality, being a 15 digit serial number known as International Mobile Equipment Identity (IMEI) which is issued by Global System for Mobile Communications Association (GSMA) which maintains a global central database containing numbers of millions of mobile devices, ie mobile phones, tablets, data cards etc known as IMEI Database. That globally the theft of mobile devices and proliferation of counterfeit and illegal devices became a main concern for regulators.

[4] In this region, the ***East Africa Communications Organization*** (EACO) where Kenya is a member together with 5th, 6th and 7th respondents agreed that the mobile service operators within the member countries would implement an Equipment Identification Register (EIR). The first phase of netting out stolen and counterfeit devices was successfully executed in collaboration with the MNOs which resulted in the switch off of 1.89 million illegal mobile handsets by 30th September, 2012 through denial of service. This was not without hindrance as well, as opposition by some mobile handset dealers emerged when they filed a case in the High Court being **HCCC No 257 of 2012, Omar Guled vs. Communications Commission of Kenya & Others**. However, the court upheld the mandate of the appellant to superintend the switch off of counterfeit and illegal phones and thus far the exercise of switching off went on smoothly.

[5] Having done so, it was explained by the appellant that the purveyors of counterfeit devices became more high-tech and started cloning genuine IMEI numbers to the counterfeit devices which made detection harder. That meant such counterfeit devices appeared as genuine when checked against the whitelist of GSMA IMEIs database and in case of switch off, it became harder to identify the genuine device from the fake ones. Then in addition to the cloning of genuine IMEIs the appellant was faced with proliferation of SIM boxing which became the next frontier for the war against counterfeit devices. Due to ease of communication over the internet, most international calls travel as an internet packet and is changed to a voice call at the destination. Thus, the SIM box operators though not licensed by the appellant to provide communication services, found a way of entering into international interconnection agreements with international carriers and illegally terminate international calls at local call termination rates.

[6] The effect of all this, was that SIM boxing operators evaded licence fee payments in contravention of ***Section 24 (1)*** of **KICA**; that they also do not pay the attendant taxes for terminating international traffic within Kenya resulting in huge loss of revenue for the country; the only records that are held by the local operators from a call arising out of SIM boxing is the local number used in the activities making SIM boxing a conduit for criminal activities as the real origin of the voice calls is untraceable. In addition, the appellant received complaints from its counterparts within the East Africa bloc, in particular Rwanda that SIM boxing operation in Kenya are being used to terminate international traffic, resulting in loss of revenue for the said country.

[7] Taking the foregoing challenges into consideration, the appellant as the regulator, engaged the stakeholders, the mobile network

operators (MNOs) and other stakeholders to create a DMS system that can: -

a) Define a whitelist of IMEIs which should access GSM services.

b) Identify counterfeit devices.

c) Identify substandard goods which have not met the type approval requirement.

d) Identify and distribute information about mobile phones reported lost and/or stolen to all service providers; and

e) Identify instances of SIM boxing operators.

To this end, the appellant stated the proposed installation of DMS was to interact with the relevant government agencies, including the Anti-Counterfeit agency and the mobile network operators (MNOs); that the appellant had requested the MNOs to nominate four officers to work with the contractor in the implementation of the project which was planned to kick off after the receipt of the nominees of the 5th, 6th and 7th respondents; that during those meetings with MNOs, and the appellant as the regulator, it was agreed that in order to address all the concerns raised, technical subcommittees be formed. That committees were formed to deal with technical, consumer and regulatory issues and they were to continue with further consultations to address all the issues of concern, including the privacy of data; interruption of network and issues relating to consumer rights.

[8] It is common ground that some meetings were held with stakeholders and key actors in the communication industry to discuss the process of implementation. Nonetheless what seems to have troubled the 1st, 5th, 6th, 7th 8th and 9th respondents including some human rights activists which led to the filing of suit before the High Court, was a letter by the appellant dated 10th October, 2016 and in particular the following: -

"DMS will facilitate the collection of information on IMEI, IMSI and MSISDN of mobile cellular end-users. The system will then enable the identification of illegal end-users'terminals, which will be listed on the DMS whitelist.

You will be expected to provide the contractor appointed by the Authority with access to information on the IMEI, IMSI and MSISDN of the subscribers on your network. Further, you will be expected to facilitate the establishment of connectivity between the DMS and your system. To achieve this, you will be required to install and maintain a dedicated link between your mobile cellular system and the DMS located at CA Centre Waiyaki Way. Further, DMS will require direct connection to your HLR and EIR and this link will be setup and maintained by the Authority. The Authority will also require rack space to install DMS is available in the "Tender Document for Device Management System" at our webpage; http;www.ca.go.ke/index.php/tenders."

[9] Also a letter dated 31st January, 2017 addressed to the 7th respondent did help to fuel the discomfort of the same respondents in regard to the proposed installation of DMS. It stated in a pertinent paragraph as follows: -

"… This is to confirm that CA DMS Technical Team will be visiting your core network facility at Safaricom on Tuesday, 21st February, 2017.

The purpose of the visit is to survey and discuss with your technical team the integration of the DMS and your network. The key highlights of the visit will be on the following matters;

I. Technical architecture of connectivity between DMS and your system to access information on the IMEI, IMSI, MSISDN and CDRs of the subscribers on your network;

II. The point(s) of connection for the dedicated link between your system and the central DMS servers located at CA Centre Waiyaki Way;

III. Rack space to install the DMS node at your premisesand clean power supply; and

IV. Any other technical matters that may arise

Further, and as agreed at the said meeting, your technical team should familiarize themselves with DMS Block Diagram and Integration Requirements forwarded to you on 13th January, 2017 and seek any clarifications on the same before the date of our visit"

[10] A petition was filed by ***Okiya Omtatah Okoiti*** (1st respondent) and all the other respondents leapt into the cause to challenge the implementation of the above project while citing several provisions of the Constitution that the proposed installation of DMS would contravene. It was alleged that the appellant did not exhaust the requirement of consultation and public participation with key stakeholders especially discussions; on the setting up of Legal, Regulatory and Consumer Affairs Committees to discuss the impact on networks and consumers and technical assessment of the design to address the numerous concerns that were raised by the stakeholders. Further it was claimed that the installation of the MSD would amount to infringement of the right to privacy, fair administrative action, and property and consumer protection rights that are protected in the Constitution.

[11] In the said petition, the following prayers were sought: -

"(a) Declaration that the impugned actions of the 1st and 2nd Respondents have threatened and violated the Constitution of Kenya, 2010.

(b) A declaration that the 1st Respondent's decision (communicated through the 1st Respondent's letters dated 31st January 2017 and 6th February 2017, both referenced as CA/LCS/1600/Counterfeit Devices/Vol. II, addressed to the 1st, 2nd and 3rd Interested Parties) to contract the 2nd Respondent to secretly set up the Device Management System (DMS) which has the capacity of spying on Kenyans, is unconstitutional and, therefore, null and void.

(c) A declaration that any vendor contracts between the 1st and 2nd Respondents, or between the 1st Respondent and any other party, associated in any way with the Device Management System (DMS) are unconstitutional and, therefore, null and void ab initio.

(d) A declaration that pursuant to Article 226(5) of the Constitution of Kenya, 2010 officials of the 1st Respondent who directed or approved the use of public funds on the DMS contrary to law or instructions, are liable for any loss arising from that use and should make good the loss, whether the officials remain the holders of the office or not.

(e) An order quashing the 1st Respondent's letters dated 31st January 2017 and 6th February 2017, both referenced as CA/LCS/1600/Counterfeit Devices/Vol. II, addressed to the 1st, 2nd and 3rd Interested Parties.

(f) An order quashing any vendor contracts between the 1st and 2nd Respondents, or between the 1stRespondent and any other party, associated in any way with the Device Management System.

(g) An order compelling the 2nd Respondent to refund any monies the 1st Respondent has paid to the 2nd Respondent pursuant to any vendor contracts between the 1st and 2nd Respondents, or between the 1st Respondent and any other party, associated in any way with the Device Management System (DMS).

(h) A permanent order of prohibition prohibiting the Respondents, whether by themselves, or any of their employees or agents or any person claiming to act under their authority from proceeding to implement the Device Management System (DMS) or, in any way whatsoever, to do anything, including installing on the networks of the Interested Parties, or any other telephony infrastructure or network, any gadget or equipment that have the capacity for spying, snooping, shadowing, investigation, scrutiny, inspection, observation, following, monitoring, reconnaissance, tailing, staking out, or in any way whatsoever or howsoever interfering with the privacy of members of the Kenyan public through communications surveillance technologies used to monitor or snoop on the population.

(i)An order that pursuant to Article 226(5) of the Constitution of Kenya, 2010, the 1st, 3rd and 4th Respondents should recover any loss arising from the DMS project from officials of the 1st Respondent who directed or approved the use of public funds on the DMS contrary to law or instructions, whether the officials remain the holders of the office or not.

(j) An order that the costs of this suit be provided for".

[12] The petition was opposed by the appellant, in a replying affidavit sworn by ***Mr. Francis Wangusi***, the then managing director. It was stated that the appellant was charged with the constitutional and statutory mandate of regulating the communication sector as envisaged under ***Article 34*** of the Constitution and ***Section 3*** of the **Kenya Information and Communication Act**; that appellant is responsible for facilitating the development of information and communication sectors in Kenya which include: -

a) Licensing all systems and services in the communications industry including telecommunications, postal, courier and broadcasting;

b) Managing the country's frequency spectrum and numbering resources;

c)Facilitating the development of electronic commerce;

d)Type approving and accepting communications equipment meant for use in the country;

e) Protecting consumer rights within the communication industry and

f) Managing competition within the sector to ensure a level playing ground for al industry players.

[13] In that regard, and pursuant also to other international and regional obligations, treaties and agreements that Kenya has signed, the appellant is obliged to upgrade its systems to continuously curb the menace of theft of mobile devices and proliferation of counterfeit devices or illegal devices which is the concern of all. To address those challenges, it was necessary for the applicant to create a centralized Equipment Identification Register (EIR) which was the DMS which squarely fell within the appellant's mandate under the Constitution and the Statute. The appellant denied the allegations that there was no stakeholder participation while stating that mobile service providers including the respondents and other stakeholders were engaged in meetings and it was generally agreed that there was need to detect all devices, isolate illegal devices and deny them service and mop up illegal devices in Kenya. After those discussions where there was consensus, the appellant embarked on a search by way of open tender of a supplier who could implement the DMS and create a system that could define and identify counterfeit devices and substandard goods, reported lost or stolen devices and instances of SIM boxing operations that had infiltrated the industry and were evading payment of licences and taxes.

[14] As regards the allegation of eavesdropping or infringement of privacy, it was stated that the installation of the system the mobile station integrated subscriber directory number (MSISDN), a number assigned to each subscriber by a mobile service provider on behalf of the appellant does not create an automatic access to the call data records (CDR) or content of such call concerning any mobile number and the access that was requested from the mobile operators EIR's and home location register was for purposes of identifying the IMEI, IMSI and MSISDN for each device. Moreover, the law permits the appellant to also hold consultations with other government agencies such as the ***Kenya Bureau of Standards*** (KBS), Anti- Counterfeit Agency, the ***Kenya Revenue Authority*** (KRA) and the National Police Service which is merely complimentary but does not interfere with its independence. The appellant denied that there was any intention to eavesdrop or interfere with the consumer's communication privacy.

[15] As regards the orders sought, the appellant contended that after competitive bidding, the second respondent was contracted to design, supply, deliver, install and commission the DMS and that mobile service providers were invited to nominate persons from their organization to the committee on the implementation of the DMS as agreed at a meeting held on 20th January, 2016.

Mr. Wangusi stated that some of the mobile service providers nominated persons from their organisations to the Committee on the implementation of the DMS while others like the ***Safaricom*** asked for more consultations. He stated that the appellant held further consultations with the various mobile service providers and other stakeholders, and that the design which was annexed to the 1st respondent's supporting affidavit was not final, and that the scope of data required by DMS was to be defined and shared with operators.

[16] Furthermore, the appellant was planning to enter into discussions to align the overlapping type approval with the Kenya Bureau of Standards and to form working groups, such as Technical, Regulatory and Consumer Affairs. Most importantly he stressed that the DMS is at the design stage, hence, the petition

before the High Court was premature and it was not true to make unfounded allegations that this was a guise to access peoples calls and mobile providers databases; that the allegations of snooping were at best premised on misinformation, hypothetical and denied the alleged violation of constitutional rights. Also, he stated that CAK is yet to respond to issues raised and that it is currently in discussion with various stakeholders and no decision has been taken. In conclusion it was emphasized that the temporary orders of injunction that had been issued interfered with the appellant's mandate to monitor compliance as per the Act, and that DMS is not a new policy but a continued upgrade of the system so as to control or stop proliferation of illegal devices. He averred that DMS can only access information on a mobile service provider network that it is authorized to access by the mobile service providers itself and that it is a clean-up process of illegal devices which commenced way back in 2011.

[17] The petition was supported by ***Broadband Communications*** (2nd respondent) who relied on an affidavit sworn on 22nd March, 2017 by the ***Chege Nganga***, their designated project manager for the implementation of the DMS project. He claimed that the system hardware had been delivered to CAK's premises and that the suppliers are already demanding payment, hence there is likelihood of prejudice being occasioned to the 2nd Respondent. He went on to state that the system will benefit Kenya's economy by blocking the use of illegal mobile devices, minimizing theft of mobile devices, blocking use of counterfeit mobile devices, stop sim boxing and cut revenue leakages from mobile operators. Moreover the DMS is incapable of spying on the calls or SMS's or mobile money transactions as shown by a letter from the manufacturer of the device stating its capabilities; that once installed, the system will be handed over to the appellant who will solely be responsible for granting 2nd respondent access for maintenance purposes only and that the 2nd respondent will not have an independent or unsupervised access to the system or data. On the prejudice to be suffered it was stated that the appellant risks losing **US$1,878,223.45** and the 2nd respondent would similarly risk incurring a monthly loss of **US$10,044.89** as a consequence of the orders that were granted.

[18] On behalf of **Safaricom,** (7th respondent) ***Mercy Ndegwa***, the head of Regulatory and Public Policy-Corporate Affairs Division swore the Replying Affidavit on 13th June, 2017 stating that: -

"(i) Safaricom was a leading communication company in East and Central Africa with over 25.1 Million subscribers;

(ii) its services include voice calls, data and Mobile Cash Transfer (M-pesa) and from subscriber to subscriber.

(iii) On 20th January 2016, CAK invited the parties to discuss the proliferation of counterfeit handsets in the country and to her knowledge on the day of the meeting, CAK had an International Tender (No. CA/PROC/OIT/27/2015-2016) for the Design, Supply, Delivery, Installation, Testing, Commissioning and Maintenance of a DMS and that the second Respondent was awarded the tender in partnership with a third party entity, Invigo OffShore Sal of Lebanon. In this regard CAK wrote to 5th, 6th and 7th respondents stating that it intended to install a DMS on mobile cellular networks to combat the proliferation of illegal communications end-user terminals including sim boxes."

[19] However, between January, 2016 and October, 2016 the appellant did not convene any meeting or engage ***Safaricom*** on the design of the system but rather only opted to communicate the specifications and design through the letter dated **10th October, 2016**. In response to the said letter, ***Safaricom's*** then Chief Executive Officer, ***Mr. Bob Collymore,*** responded vide a letter dated **17th October, 2016** raising among other issues, privacy, confidentiality and consumer concerns arising from the fact that its consumers' personal information was going to be in the custody of a third party (2nd Respondent). The letter also raised security concerns on the installation of the DMS, which would have to be addressed prior to the commencement of the project. In response, she avers, the appellant called a pre-implementation meeting which took place on **26th October 2016**. In the said meeting, she states, CAK proposed two committees to discuss the matter, namely, technical and regulatory. Further, she avers, the interested parties proposed a consumer committee which would among others engage the public and consumer organizations on consumer related concerns such as privacy and consumer awareness. The appellant convened a technical meeting on **23rd November, 2016**, in which the 5th, 6th and 7th respondents raised the same concerns on privacy and consumer awareness of the project and upon conclusion of the meeting it was their understanding that DMS design were to undergo further discussions on the issues raised. She further states that on **13th January, 2017**, CAK wrote a letter to the third interested party indicating that they would supply the third interested party with a network block diagram showing how the DMS would interconnect with the core network. This was followed by another letter on **25th January, 2017**, where by it was agreed that a regulatory discussion of the project cannot be done without the conclusion of the technical discussion of the project; but contrary to what was agreed, on **31st January, 2017**, the appellant wrote a letter to ***Safaricom*** stating that its DMS technical team shall visit their network facility on **21st February, 2017** to survey the integration of the DMS to their network, and to discuss the same with the technical team.

[20] The fears by Safaricom were stated vide a letter dated **17th February, 2017** that; a technical assessment was still required to be

done prior to installation so as to pave way for the Legal, Regulatory and Consumer Affairs Committees to discuss the impact on the networks and consumers to clarify whether the 2nd respondent would have unfettered access to the consumers' call data records, location information, credit card and M-Pesa information, identification information and SMS information, which basically equates to all the records of any consumer with a registered mobile device; that their subscribers would desist from using their devices, in effect reversing the progress made in making communication easier for subscribers; that the decision to install the device without consultation was arbitrary, and, that the law does not grant the appellant power to arbitrarily interfere with communication devices by tapping, listening to, surveillance or intercepting communications related data. In their view the appellant's actions were contrary to **Article 10 (2)** of the Constitution, and that it does not state that the current measures in place to curtail counterfeit devices taking into account the Anti-Counterfeit Act, the KBS or stopping the items at the points of entry. She avers that the installation of DMS requires consultations in line with rights under **Articles 31**, **47** and **40** of the Constitution. This position was reiterated by **Article 19**, the 9th respondent.

[21] After hearing the parties and duly considering the submissions and authorities, the learned trial Judge rendered the judgment on 19th April, 2018 granting the following orders which he customized according to what he referred to as the justice and circumstances of the case. This is what is stated in the Judges own words.

"…I have however considered the reliefs the Petitioner has invited this court to grant. However, I think this is a proper case for this court to fashion appropriate reliefs as the justice and circumstances of the case demand. This Court is empowered by Article 23 (3) of the Constitution to grant appropriate reliefs in any proceedings seeking to enforce fundamental rights and freedoms such as this one. Perhaps the most precise definition of "appropriate relief" is the one given by the South African Constitutional Court in *Minister of Health & Others vs Treatment Action Campaign & Others*] thus: -

"....appropriate relief will in essence be relief that is required to protect and enforce the Constitution. Depending on the circumstances of each particular case, the relief may be a declaration of rights, an interdict, a mandamus, or such other relief as may be required to ensure that the rights enshrined in theConstitution are protected and enforced. If it is necessary to do so, the court may even have to fashion new remedies to secure the protection and enforcement of these all important rights....the courts have a particular responsibility in this regard and are obliged to "forge new tools" and shape innovative remedies, if need be to achieve this goal."

I fully adopt this definition of "appropriate reliefs" and shall deploy it in my disposition of this suit. Arising from the findings of evidence, conclusions of facts and law, constitutional and statutory interpretations and various pronouncements of law, I have reached above, I make the following orders: -

***a) A declaration** be and is hereby issued that policy decisions or Regulations affecting the Public must conform to the Constitution and the relevant statute in terms of both its content and the manner in which it is adopted and failure to comply renders the policy decision, Regulation or guideline invalid.*

***b) A declaration** be and is hereby issued decreeing that the decision, policy or regulation seeking to implement the DMS System was adopted in a manner inconsistent with the provisions of the Constitution, Section **5 (2)** of KICA and the Statutory Instruments Act, hence the said decision, policy and or regulation is null and void for all purposes.*

***c) Further and or in the alternative a declaration** be and is hereby issued decreeing that the decision, policy and or regulation seeking to implement the DMS System was adopted in a manner inconsistent with the Constitution, Section **5A (2)** of KICA and the Statutory Instruments Act in that there was no adequate public participation prior to its adoption and implementation with the first, second and third interested parties and further the subscribers of the first, second and third Interested Parties were not engaged at all in the public consultations, hence the same is null and void for all purposes.*

***d) A declaration** be and is hereby issued decreeing that the first Respondent was obligated to craft and implement a meaningful programme of public participation and stakeholder engagement in the process leading to the decision, policy and or regulation or implementation of the DMS System.*

***e) A declaration** be and is hereby issued declaring that the first Respondents request and or purported intention and or decision and or plan contained in its letter dated **31st** January 2017 addressed to the first, second and third interested parties seekingto integrate the DMS to the first, second and third interested parties networks to inter alia create connectivity between the DMS and the first, second and third Interested Parties system to access information on the IMEI, IMSI, MSISDN and CDRs of their subscribers on*

their network is a threat to the subscribers privacy, hence a breach of the subscribers constitutionally guaranteed rights to privacy, therefore unconstitutional null and void.

***f) A declaration** be and is hereby issued declaring that the first Respondents decision to set up connectivity links between the DMS and the first, second and third Interested Parties networks communicated in its letter dated **6th** February 2017 is unconstitutional, null and void to the extent that it was arrived at unilaterally, without adequate public participation and that it a threat to the right to privacy of the first, second and third interested parties subscribers and a gross violation of their constitutionally and statutory protected consumer rights.*

***g) An order of prohibition** be and is hereby issued prohibiting the first Respondent, its servant or agents from implementing its decision to implement the DMS system to establish connectivity between the DMS and the first, second and third Interested Parties system to access information on the IMEI, IMSI, MSISDN and CDRs of their subscribers on their network.*

h) No orders as to costs."

[22] The appellant was aggrieved by the said orders; it consequently filed an appeal raising a total of thirty-two (32) grounds of appeal which are prolix and repetitive. We intend therefore to summarize them following the line of arguments adopted in the appellant's written and oral submissions made in court during the hearing which were; that the learned Judge erred in law and fact by failing; to hold that the petition was premature/or hypothetical; by taking into consideration matters not pleaded in the petition before it; to consider and answer the critical question as to whether the installation of the Device Management System (DMS) threaten or violate the right of privacy of subscribers; whether the Judge appreciated the nature, content and import of the appellant's letter dated 31st January, 2017; the statutory mandate of the appellant; the standard and threshold of public participation; whether the Statutory Instruments Act is applicable to the appellant's decision on the DMS; was the introduction of the DMS inconsistent with consumer rights as guaranteed by law and finally whether there was breach of the provisions of the **Fair Administrative Action Act** in introducing the DMS.

[23] During the plenary hearing, the appellant was represented by ***Mr. Wambua Kilonzo*** led by ***Prof. Githu Muigai SC***. They relied on the appellant's written submissions with some oral highlights. It was the appellant's submission that the Judge misdirected himself when he held that the petition before him was not hypothetical on account that the 1st respondent had a standing to seek relief in that he had alleged that his right to privacy was threatened with violation. According to counsel for the appellant this was a misdirection because the doctrine of *locus standi* and the doctrine of ripeness are two different matters. This was because the 1st respondent and other parties who supported the petition did not provide any supporting evidence of the existence or possibility of breach of fundamental rights of any person. Moreover there was no decision capable of challenge in the proceedings since the consultation to agree on the architecture and implementation and installation of the proposed DMS and the engagement between the parties was still ongoing.

[24] Counsel went on to submit that for an issue to be justiciable, there must be a real identifiable and likelihood of a breach or a threatened breach of a right. It is also an accepted tenement of law that a court of law is not expected to engage in abstract arguments merely out of apprehension. The case of **John Harun Mwau & 3 Others vs. Attorney General & 2 others [2012] eKLR** was cited to bolster the proposition that a court cannot rely on hypothetical matters as there must be a real threat. On standing, counsel submitted that a court is not a debating society making it the business of court to decide matters predicated on newspaper cuttings and mere allegations that the government will start snooping on their communication which was not based on any tangible evidence. Counsel relied on the case of **Wanjiru Gikonyo & 2 Others vs. National Assembly of Kenya & 4 others [2016] eKLR** where it was held *inter alia* that: -

"Effectively, the justifiability dogma prohibits the court from entertaining hypothetical or academic interest cases. The court is not expected to engage in abstract arguments. The court is prevented from determining an issue when it is too early or simply out of apprehension, hence the principle of ripeness. An issue before the court must be ripe, through a factual matrix, for determination"

[25] Taking on the grounds on whether the installation of the DMS device threaten or violate the right to privacy of subscribers, ***Mr. Kilonzo*** submitted that the affidavits of ***Mr. Wangusi*** clearly explained the genesis of the idea and why it was imperative for the appellant as the sole regulator of the communication sector to perform its constitutional, statutory, international and regional mandate. Counsel submitted that the Judge created his own case not founded on factual and technical details that were provided in the affidavits sworn by ***Mr. Wangusi*** which were not controverted when he held that the DMS referred to interception of calls, *SMS*

and data bundles without an iota of evidence of how that was going to happen. Although the device had been procured, the methodology of its use and interaction with other MNOs was still under discussion and nothing was produced in evidence in support of the petition to inform any of the conclusions reached by the Judge on alleged spy capabilities

of the proposed DMS. Stopping the installation of the system has meant that the cartels who extort and demand money for the call ends cannot be blocked and cloning of counterfeit devices without detection have continued unabated. The orders issued have interfered with the specific mandate of the appellant as the regulator to issue a type approval certificate for a specific model of communication equipment and to licence the operators.

[26] Counsel also faulted the Judge for finding that there was inadequate public participation prior to the process leading up to the acquisition and the attempt to install the DMS system. In this regard counsel pointed that there was a lot of uncontroverted information of how the appellant had relentlessly engaged the industry in the fight against illegal and counterfeit devices from the year 2012. Further counsel submitted that the Judge went beyond the issues that were pleaded in the petition before him by introducing consumer rights under **Article 46** of the Constitution and the **Consumer Protection Act** when the said article requires the goods and services offered to be of reasonable qualities, hence it was also applied out of context. According to counsel, the DMS project serves to protect the consumer from the menace of illegal devices which ***"affect economic growth and intellectual property rights, impede innovation, are hazardous to health and safety and have an impact on the environment and the increasing amount of harmful e-waste"*** *as stated in* ***International Telecommunication Union's*** **(ITU) resolution 79 (Dubai 2014).** Counsel therefore urged that the project cannot be a violation of consumer rights, he prayed that we allow the appeal with costs.

[27] The appeal was supported by ***Mr. Ogoso*** learned counsel for the ***Cabinet Secretary, Information Communication and Technology*** and the ***Attorney General***, the 3rd and 4th respondents respectively. He did not make any submissions but wholly adopted and associated himself with the submissions made on behalf of the appellant.

[28] The appeal was opposed by the 1st respondent, ***Mr. Omtatah*** acting in person. He relied on his written submissions and made some oral highlights stating that the petition before the High Court was not hypothetical as it met the threshold of what is justiciable under **Articles 22 (1)**, **165 (3) (b)** and **258 (1)** which provides for standing in every person to institute court proceedings when a fundamental right is denied, violated, infringed or threatened; the jurisdiction to determine such rights is vested in the High Court and generally vests standing in every person to institute proceedings on any contravention of the provisions of the Constitution. According to the 1st respondent, DMS was clawing back the gain protected by the Constitution by giving the regulator powers through the back door to interfere and spy on consumer's telephone communications which contravened the right to privacy. Further the regulator did not give examples of how DMS works in other jurisdictions which is also a mandate of the police and Anti-counterfeit Agency to recover stolen and illegal mobile devices.

[29] The 1st respondent went on to argue that freedoms of all types of media is guaranteed under **Article 34** of the Constitution; that the appellant although an autonomous body cannot purport to flex its mandate to curtail guaranteed freedoms and that no statute allowed the appellant to interfere with communication by third parties. On the allegations that the Judge ruled on matters that were not pleaded, it was the 1st respondent's view that all the matters

were pleaded in regard to enactment of DMS without appropriate public participation or consultation and in contravention of the Statutory Instruments **Act 2013** and the **Fair Administrative Action Act 2015**. In this regard he cited the case of **Galaxy Paints Co. Ltd vs. Falcon Guards Ltd [2000] E.A 885** among others for the proposition that a court of law can frame issues arising from those issues that are in controversy even when not directly pleaded. The 1st respondent urged us to dismiss the appeal and uphold the decision of the High Court.

[30] Also opposing the appeal was ***Mr. Nani Muigai*** appearing for the 7th respondent. Counsel relied on the written submissions and made some oral highlights. On the question of whether the petition was hypothetical and or premature, counsel submitted that the appellant had engaged the 7th respondent alongside other MNO's on the roll out of the DMS in meetings held on 26th October, 2016 and 25th January, 2017 where their client raised key issues that included privacy, confidentiality, consumer concerns as well data security arising out of the installation of the DMS. Notwithstanding the aforesaid concerns the appellant informed all the MNOs that their contractor was going to integrate DMS to access information from the subscribers of their networks. Counsel conceded that there were discussions that were on going where it was suggested that technical committees be formed to deal with the issues and concerns raised, but *alas,* the appellant went ahead to undertake implementation before addressing those concerns of the stakeholders. The 7th respondent hoped that the appellant would address the issues raised in order to protect its subscribers' data

from manipulation and other attendant safeguards.

[31] To further demonstrate that the petition was not hypothetical, counsel for the 7th respondent pointed out that the appellant had invited bidders in an international open tender to bid for the installation of the DMS system whose key criterion was for the system to have the ability to track the location of the mobile device, access to various sensitive components and records of customer devices at any time which include call data records (CDRs), billing systems and home location registers and records of MNO's. That other third parties such as the ***Kenya Revenue Authority***, ***Kenya Bureau of Standards*** and the ***National Police Service*** would have access to this information; that the process of installation and integration started before all the concerns were addressed and that there was no public participation on the implementation. To reinforce this submission, counsel relied on the case of **Coalition for Reforms and Democracy & Others vs. Attorney General, Petition No 628 of 2014 [2015] eKLR**, which dealt with the interpretation of **Articles 22, 165 (3) (d)** and **258** of the Constitution that: -

"....A party does not have to wait until a right or fundamental freedom has been violated, or for a violation of the Constitution to occur, before approaching the court …'

According to counsel in order to secure the privacy of subscribers, it was necessary for the appellant with stakeholders to develop a regulatory framework to protect not only the privacy of the subscribers but also the MNOs as well as the general consumers. Counsel urged us to dismiss the appeal

[32] Opposing the appeal also was ***Mr. Manases*** for the ***Kenya Human Rights Commission,*** who reiterated the submissions by the 1st and 7th respondents. He emphasized that there was a real likelihood of threat to breach of fundamental rights to privacy as DMS was likely to spy on private communication. If the appellant wishes to mop up illegal mobile devices it has all the IMEA numbers which can be used to identify stolen and counterfeit devices. Moreover, it is the Anti- Counterfeit Authority and the police who have the mandate to deal with counterfeits and the appellant was merely overstepping its mandate by intruding into surveillance which threatens the right to privacy which is duly protected under **Article 31** of the Constitution.

[33] The 2nd, 5th and 6th respondents did not participate in the hearing of this appeal although they were duly served with the hearing notice.

[34] We have considered the appellant's appeal which was supported by the 2nd and 3rd respondents as well as the 1st, 7th and 9th respondents' opposition as advanced in their pleadings and oral submissions, list of authorities and also the oral submissions made on behalf of the ***Kenya Human Rights Commission***. This is a first appeal, although we recognize no oral evidence was adduced, we nonetheless have a duty to re-evaluate and re-analyse all the material that formed

part of the pleadings and affidavit evidence which informed the decision of the learned Judge, the subject matter of this appeal. See the case of **Abok James Odera T/A A.J Odera & Associates vs. John Patrick Machira T/A Machira & Co. Advocates [2013] eKLR**, in which this Court stated as follows:

"This being a first appeal, we are reminded of our primary role as a first appellate court namely, to re-evaluate, re-assess and reanalyze the extracts on the record and then determine whether the conclusions reached by the learned trial Judge are to stand or not and give reasons either way."

[35] That said and as indicated in the opening paragraph, arising from our own re- evaluation of the matters before the trial court as demonstrated by the above summary, we think the following issues fall for our determination. That is; whether the suit was hypothetical and or premature; whether there was adequate public participation in the proposed design and installation of the DMS; whether the installation of the DMS threatened the consumer's rights to privacy and therefore a breach of the Constitution; whether the pleadings disclosed any violation of the respondents' or consumers' rights or the Judge construed a different cause of action; and whether the mandate of the appellant as the communications regulator was misapprehended by the Judge and thereby curtailed. We think in the circumstances of this matter, it will be prudent to deal with all the issues together. We however acknowledge that the issue of **ripeness** of the matter, cuts across and it has a strong bearing on all the other issues.

[36] According to the appellant, the matter was not ripe for litigation as there were on going consultations with stakeholders that involved technical aspect of the installation of DMS and this was evidenced by various correspondence and minutes of meetings that were held by the parties. On the part of the 1st, 5th, 6th, 7th and 9th respondents and the ***Kenya National Human Rights Commission***,

there was a threat to violation of consumers' right to privacy which gave rise to a cause of action as the right so threatened is protected in the Constitution.

[37] The case as pleaded in the petition filed by the 1st respondent is with respect slovenly drawn; it is made up of generalized allegations that are wholly predicated on unsubstantiated statements taken from newspaper reports and statements made by unnamed technical experts. This is just a glimpse of one such paragraph 8 of the petition to wit;

"The decoy the government is posting to justify the system of eavesdropping on private communications and which will sit on all mobile phone networks, is that the DMS is required to monitor and identify stolen handsets, counterfeit phones, and devices that have not been type approved by the regulator. However the government is silent on the systems capabilities for spying on calls and texts and also reviewing all mobile money transactions which extend beyond what is being stated, and how it will protect the privacy of individuals once the information is collected by the 2nd respondent (a third party entity) and shared with third parties, including law enforcement and the government's other agencies."

[38] The 1st respondent states in the supporting affidavit that the source of his fear was that the appellant was going to curtail the freedoms guaranteed in the Constitution. This fear was based on the stories published in the banner headlines of the leading newspapers for which he stated in Paragraphs 6 and 8 as follows;-

"That both the application and petition raise a matter of grave public concern, evidenced by the fact that when the issue broke out, both the Daily Nation and the Standard, Kenya's two main national newspapers, published the story as their banner headlines for the day

"That the facts stated establish a sufficient case with a high possibility of success in respect to the applicants/ petitioners' claims, and that further there is an overarching requirement of justice that orders sought be granted".

To this end, the 1st respondent annexed newspaper cuttings with sensational headlines like "**Bold plan to spy on all calls, texts rolled out from Tuesday next week, if mobile firms comply, someone other than your provider will be able to access your call, text and money transfer data …"**Daily Nation of 17th February, 2017. The Standard also published this; "**Big Brother could start tapping your calls, texts from next week"**

[39] We agree the probative weight to be given to a statement of facts contained in newspaper cuttings, required the maker of the statement to appear in court and be subjected to court room processes for that statement to be admissible in evidence. See the case of **Independent Electoral and Boundaries Commission (IEBC) vs. National Super Alliance (NASA) Kenya & 6 Others [2017] eKLR**

where this Court stated as follows on the probative value of evidence contained in newspapers: -

"On our part, having considered the evidence on record and the law relating to admissibility and probative value of newspaper cuttings, we find that a report in a newspaper is hearsay evidence. We are conscious of Section 86(1) (b) of the Evidence Act which provides that newspapers are one of the documents whose genuineness is presumed by the court. This section prima facie makes newspapers admissible in evidence. However, a statement of fact contained in a newspaper is merely hearsay and therefore inadmissible in evidence in the absence of the maker of statement appearing in court and deposing to have perceived the fact reported…"

This exposition of the law is the one that guides the courts on the admissibility and the probative value of newspaper reports. As far as the framing of the issues are concerned, we have already demonstrated that the petition was not elegantly drawn. We are also conscious of the cardinal rule in construction of pleadings, especially in our adversarial system of litigation that a party is bound by their pleadings, which is meant to protect the other party who should not be ambushed with new claims in the course of a hearing. These are well beaten principles which were articulated quite early in the case of **Anarita Karimi Njeru vs. Republic (1976-1980) KLR 1272** that a person seeking redress from the High Court on a matter which involves a reference to the Constitution, should set out with reasonable degree of precision in particular how the alleged acts amount to infringement of the person's constitutional rights. The petition and the supporting affidavits were based on allegations of what was feared might happen, conjectures or at best unconfirmed sources of information. For instance, Para 9 of the petition states: -

"Technical experts have pointed out that while there would be no concern over the access to the International Mobile Subscriber Identity, which is a unique number identifying a mobile phone subscriber, other access like home location register raise concerns"

It is not indicated who these technical experts are and the whole petition is replete with such sweeping allegations.

[40] Be that as it may, we have given this matter a broader view as the pleadings by the 1st respondent were not the only ones the Judge relied on. The 1st appellant's case was augmented along the way by the averments made in the supporting affidavit of ***Mercy Ndegwa*** on behalf of the 7th respondent. Although this may seem like an ambush to the appellant we find that they responded to that affidavit extensively. Moreover, we have also taken into account the overarching principle in the administration of justice that is to do substantive Justice which provisions are awash in our laws. It is prudent on our part to consider and determine all the issues raised in this appeal. See **Chaskalson, J.** In the South African case of **Pharmaceutical Manufacturers Association of South Africa & Another: exparte President of the Republic of South Africa & Others (CCT) 31/99) [2000] ZACC 1; 2000 (2) ZA 674:**

"***Review power of the court is no longer grounded in the common law, and therefore susceptible to being restricted or ousted by legislation. Instead the Constitution itself has conferred fundamental rights to administrative justice and through the doctrine of Constitutional supremacy prevented legislation from infringing on those rights. Essentially, the clause has the effect of 'constitutionalizing' what had previously been common law grounds of judicial review of administrative action. This means that a challenge to the lawfulness, procedural fairness or reasonableness of administrative action, or adjudication of a refusal of a request to provide reasons for administrative actions involves the direct application of the constitution."***

[41] In this regard we have considered in great detail the matters contained in an affidavit sworn on **8th June, 2017** by ***Mercy Ndegwa*** which was supporting the petition. In it, she attached copies of the letters alluded to in **paragraphs 8 and 9** of this judgement. Those letters, in our view, formed the foundation of the petition before the High Court and not, the unsupported allegations stated in the petition. The aforesaid letters were followed with others especially the letter dated 6th February, 2017 in which the appellant stated that it had commenced the DMS project installation and integration, and requested that the 7th respondent grants the 2nd respondent access to its site for installation.

[42] The record shows that the 7th respondent responded to the said letter stating that a technical assessment was still required to be done prior to the installation of DMS so as to pave way for the legal, regulatory and consumer affairs committees to discuss the impact on the networks and on the consumers. The

letter dated the 17th February, 2017 requested for a meeting to discuss the proposed technical assessment of the design and the possibility of an alternative design that would address the issue of counterfeit devices on the network. Nonetheless as stated by ***Mr. Wangusi*** in his replying affidavit, by the time the appellant received this letter, *the horses had bolted*, as the matter was filed in court and interim orders issued restraining the appellant from proceeding with the installation of DMS.

[43]The question we have to answer is whether the matter was ripe for litigation. It is clear to us that both sides of the divide looked at it differently. To the

appellant, the letter dated 31st January, 2017 stating that the **CA DMS** Technical Team will visit the 7th respondent's site on 21st February, 2017 **"to survey and discuss with your technical team the integration of the DMS and your network"** merely meant a survey or to configure the DMS and discuss technical issues with a view for further processing by the thematic committees that were formed, whereas to the respondents it amounted to a threat to a fundamental right to freedom of privacy which they did not have to wait for it to occur, before invoking the provisions of **Article 22** of the Constitution had occurred. This is what **Article 22** provides: -

"Every person has 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 threatened"

Article 258 provides: -

"Every person has the right to institute court proceedings claiming that the Constitution has been contravened or is

threatened with contravention"

The specific right to privacy is provided under **Article 31** which provides that;

"Every person has the right to privacy, which includes the right not to have: -

a) Their person, home or property searched;

b) …

c) …

d) The privacy of their communication infringed"

[44] In determining this issue of ripeness, the learned Judge went into a very detailed analysis of what constitutes access to information, right to privacy in communication, data protection and a lot of other issues ranging from international treaties and human rights instruments. In respect of the specific conclusion on ripeness of the matter, he found that there was a threat to the respondents' and other consumers' right to privacy of communication. This is what the Judge stated in his own words;

"The letter dated 31st January 2017 referred to earlier clearly states the purpose of the DMS system that is to "to access information".

Accessing such information can only be lawful if it falls within the permitted parameters of Section 27A of KICA. Accessing mobile telephone subscriber's information in a manner other that as provided under the law inherently infringes the right to privacy, a fundamental right guaranteed under the constitution. It follows that for the DMS system to lawful, the reason given must not only be lawful, but it must meet the Article 24 analysis test in that it must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including the nature of the right or fundamental freedom; the importance of the purpose of the limitation; the nature and extent of the limitation; 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 the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose".

[45] In arriving at the aforesaid conclusion, the Judge has been faulted by the appellant for failing to consider the detailed position given by the appellant especially the undisputed matters that are stated in the affidavits of ***Mr. Wangusi***

alluded to earlier on and by **Mercy Ndegwa**. We find some merit in this argument as the Judge overlooked the statutory mandate of the appellant which is as stated in **the Kenya Information and Communication Act No 2 of 2018** (KICA) that is *inter alia* to licence, and regulate postal information and communication services. The Judge also did not identify the actual probable evidence that led to the conclusion that DMS would intrude on privacy and even if there were issues of concerns they were still being addressed. Another key concerns that the Judge overlooked was the undisputed fact that there were acknowledged challenges in the sector which needed to be fixed. In fixing those challenges, there was a strategy which was implemented in the 1st phase where about 1.8 million stolen and counterfeit devices were netted and switched off. However the challenges escalated to another level where the purveyors of counterfeit devices became more high-tech and started cloning genuine IMEI numbers to the counterfeit devices whose detection was not possible. In addition, the appellant was also faced with proliferation of SIM boxing operators who were operating illegally without a licence or remittance of taxes in contravention of the law.

[46] We find that had the Judge considered the nature of the challenge that was being addressed, he would have arrived at a different conclusion to balance the right to protection of freedom of privacy and to allow the appellant execute its mandate while following the law and in consultation with the other players in the industry. This is fortified by the fact that the whole challenge that faced the mobile communication sector was not only a domestic issue, but one that had a bearing to regional and international obligations. The Judge went into so much interpretation of the general human rights protection, but did not give similar regard and attention to the challenges that needed to be addressed with solutions. The whole judgment was eclipsed by the interpretation that he gave to the term **"access",** which he defined as intrusion to a persons' right to privacy which we believe was well intentioned but he failed to consider the other side of the coin when he posited:-

"**The words to note in the letter dated 31st January 2017 are: - *"....to access information on the IMEI, IMSI, MSISDN and CDRs of the subscribers on your network."* These words warrant no explanation. Section 2 of KICA defines "access: - as follows: - "access" in relation to any computer system", means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system."**

[47] We think the Judge over concentrated only on the interpretation of an aspect of the term *'access'* in a narrow sense in regard to retrieving data which he took to mean intrusion of privacy to communication. He however did not consider other aspects of *'access'* such as making use of the resources to address the challenges at hand. We state this cautiously, noting that in accessing the data there was fear that the right to privacy was likely to be infringed which seems to

have preoccupied the Judge. The right to privacy is important but the issues of abuse by unscrupulous mobile operators also needed to be tackled so as to strike a balance between securing the right to privacy and dealing with the problem without infringing the right to privacy. In undertaking the DMS, which was agreed by all the parties was in pursuit of the appellant's mandate to regulate the mobile communication sector, the appellant had a duty to abide by the law. It is clear to us that there was no concrete evidence that the DMS was going to spy or intrude on private communication other than the unsupported newspaper cuttings. It is also clear to us that there were genuine issues raised by MNOs which were still being discussed.

[48] Having said that, we nonetheless acknowledge that the letters sent by the appellant to the 7th respondent created apprehensions or some panic, which were answered when the appellant stated that DMS was still being configured and discussions were underway to thrust out issues of concern raised by the 7th respondent. Unfortunately once the learned Judge issued interim orders stopping any further implementation of the DMS those issues of concern could not be addressed. This was followed by the final orders that declared DMS as null and void, thereby nipping it on the bud. The challenge that was there in the mobile communications sector remained unaddressed and this lends credence to the appellant's legitimate concern about their mandate as the regulator and the challenge of the illegal mobile operators.

[49] We recognize that courts cannot carry out the mandate of the appellant or any public body for that matter, their role is to adjudicate on concrete disputes. To this end, there was apprehension, but the same had not crystalized, as meetings with technical teams were continuing to discuss the design, the architecture, and configuration of DMS. Had the learned Judge considered the detailed averments contained in affidavits by ***Mr. Wangusi***, the response by

Mercy Ndegwa on behalf of the 7th respondent; the various correspondenceexchanged and the minutes of the meetings including by the technical committees, perhaps he would have found, as we have, that the 'access' requested was for purposes of configuring the **DMS** and not for installation purposes. Even if it was for installation, there was no credible evidence to demonstrate that the system was meant to spy on consumers' private information other than to net out the illegal operators.

[50] We repeat that there were technical issues such as a justification as to why the DMS equipment was tendered for and procured before the guidelines were agreed upon by the stakeholders. Although the tendering and procurement was not an issue, we understood that the DMS needed to be procured for purposes of building it up or configuring it with the existing infrastructures which was not the same as installation which point we think was not addressed by the learned Judge except when he construed it as evidence of threat to intrude on privacy of communication. This is how it was put in the words of the appellant's affidavit sworn by ***Mr. Wangusi*** on 5th October, 2017: -

"That further the Authority states that on the said site visit day of 21st February, 2017 proposed in the Authority's letter of 6th February, 2017 the representatives of the 2nd respondent were to meet the technical team of the 1st 2nd and 3rd interested parties on the said date for the purposes of surveying and discussing the architecture of the DMS as had been agreed in the stakeholder meetings of 25th January 2017 and conveyed in the Authority's letter dated 31st January, 2017"

[51] The appellant's explanation that consultations were not completed as the DMS was still under development and technical committees that were formed were still working was not controverted. See the exact averments by Mercy

Ndegwa as stated in paragraph 21 of her replying affidavit sworn on 8th June, 2017: -

"***That the 3rd interested party responded to the said letter dated 17th February, 2017 stating that a technical assessment was still required to be done prior to the installation so as to pave way for the Legal, Regulatory and Consumer affairs committees to***

discuss the impact on networks and consumers. The letter further requested the 1st respondent for a meeting to discuss the 3rd interested party's proposed technical assessment of the design and the possibility of an alternative design that would address the issue of counterfeit devices on the network, however the same did not elicit a response"

In response to the above, the appellant agreed that consultations were ongoing but this letter was overtaken by events because by the time it was received, there was already an order by the High Court stopping the appellant from continued implementation of the DMS.

[52] The records of the various consultative meetings held between the stakeholders and the MNOs demonstrate that there was on-going public participation. However, the final working document, call it guideline or regulatory framework on how the DMS would operate, was not agreed upon as the process of consultation was not completed. Since this process was not completed, it would be premature to decide whether public participation was adequate or not, noting that there is no known science of determining this but a consideration of several factors as stated in the High Court case of; ***In the matter of the Mui Coal Basin Local Community [2015] eKLR*** where the three-Judge bench expressed themselves as follows: -

"It is not possible to come up with an arithmetic formula or litmus test for categorically determining when a Court can conclude that there was adequate public participation. However, as we have alluded above, the Courts look at the bona fides of the public actor, the nature of the subject matter, the length and quality of engagement and the number of mechanisms used to reach as many people as possible."

See also see decision in **Doctors for Life International vs. Speaker of the National Assembly & Others (CCT12/05) [2006] ZACC 11; 2006 (12) BCLR 1399 (cc); 2006(6) SA 416 (CC)** where the constitutional court stated:

"The measure and degree of public participation that is reasonable in a given case will depend on a number of factors. These include, the nature and the importance of the legislation and the intensity of its impact on the public. The more discreet and identifiable the potentially affected section of the population, and the more intense the possible effect on their interest, the more reasonable it would be to expect the legislature to be astute to ensure that the potentially affected section of the population is given a reasonable opportunity to have a say." [Emphasis added]

[53] Having found as we have that there were some fears that lingered after the

letter by the appellant dated 31st January, 2017; although those fears were assuaged by the appellant in their response to the petition, the learned trial Judge clearly misapprehended the issues before him when he found the freedom of right to privacy of consumers was threatened and that there was no public participation. As we have stated, the DMS was still in its architectural or configuration design stage and consultations with stakeholders were on going. In our view, the orders that commended themselves to the situation was not to declare the whole DMS project null and void; it was to allow the construction of the DMS to continue while abiding by the law and ensuring protection of freedom of privacy.

[54] In the upshot, we find the appeal has merit. We therefore set aside the orders of 19th April, 2018 and substitute therefor orders that: -

(a) In exercise of its mandate of developing a DMS system, the appellant shall continue with the consultations that were ongoing with the stakeholders and MNOs prior to the filing of the petition so as to complete the technical and consumer guidelines on the DMS.

(b) The guidelines/ regulations should be subjected to public participation.

(c) For the same reasons given by the High court we order each party to bear their own costs of the appeal.

Dated and delivered at Nairobi this 24th day of April, 2020.

W. OUKO, (P)

.....

JUDGE OF APPEAL

M. K. KOOME

.....

JUDGE OF APPEAL

D. K. MUSINGA

.....

JUDGE OF APPEAL

I certify that this is a true copy of the original

Signed

DEPUTY REGISTRAR