PRESS STATEMENT

PRESS STATEMENT BY MR. FRANCIS W. WANGUSI, DIRECTOR GENERAL, COMMUNICATIONS AUTHORITY OF KENYA (CA), ON MISLEADING MEDIA REPORTS REGARDING THE REGULATORY TOOL FOR CURBING COUNTERFEIT DEVICES ON MOBILE NETWORKS

The attention of the Communications Authority of Kenya (CA) is drawn to claims in the social and local media that the Authority is implementing the Device Management System (DMS) with the express intention of monitoring and accessing private data of mobile phone users. The reports further allege that the Authority has, at the behest of government, asked mobile network operators and service providers to allow CA's agents to plant gadgets on all mobile networks that have the ability to gain access to all information on mobile devices including details on subscribers' communications such as voice calls and SMS messages, as well as mobile money transactions, in blatant breach of law. .

The Authority wishes to respond as follows:

1) The Authority has over the years deployed various systems to ensure that only authorized communications devices are in use in the market as provided for in the ICT sector law.

2) The deployment of these systems is informed by the fact that telecommunications systems and devices only work well if they comply with the prescribed technical standards. Compliance with technical standards ensures conformance and interoperability between the various systems that constitute the telecommunications network and goes a long way in addressing the challenge of illegal termination of telecommunications traffic. The law only allows type-approved and genuine mobile telecommunications equipment to be used in the country.

3) The proliferation of counterfeit devices, often illegally imported and acquired by the public, presents a serious challenge to mobile networks and subscribers. Besides compromising the optimization of mobile networks, such illegal devices degrade the quality of service available to users. The use of counterfeit devices poses a great security threat, because such devices do not provide for effective identification or traceability of network transactions/users.

SIM-boxing, which is used by unscrupulous people to illegally divert and terminate telecommunications traffic, not only poses a security threat but also leads to loss of revenue to both mobile operators and government through evasion of taxes.

4) The implementation of this system is also intended to meet the requirements of the East African Region under the Northern Corridor Integration Project Heads of State Summit, which directed each member state to deploy systems that curb illegal by-pass and termination of telecommunications traffic within the context of the 'One Network Area'.

5) It is against this background that the Authority has continued to revamp the framework for the management of illegal telecom devices in the country. Indeed the acquisition of a Device Management System (DMS) is the second phase of the initial initiative that saw Mobile Network Operators switch off all counterfeit mobile devices in Kenya in 2010.

6) Subsequently, the Authority, following extensive consultation with industry and other stakeholders including COFEK, facilitated the set up of an SMS-based mobile device verification service, through use of the "1555" short code for use by consumers in confirming the status of mobile devices before purchase. The set up of the device verification system was undertaken with the understanding that there would be a second phase that would involve deployment of a more comprehensive system that would address importation of illegal devices, pre-shipment verification of devices as well as denial of service of devices already in the market.

7) Arising from the above, the Authority is in process of deploying the second phase of the system in order to manage the menace of counterfeit devices. The system dubbed the DMS is being deployed in close consultation with the local mobile network operators. Contrary to the claims raised through COFEK, the implementation of the system is being coordinated by a team that has the involvement of the mobile network operators, CA and other relevant government agencies.

8) The DMS is a comprehensive system that is not only able to manage entry of devices into the country but equally prevent access of illegal communication devices to mobile telecommunications services. The DMS will be populated by data of all genuine devices (a whitelist), to uniquely identify each device. Once deployed, the DMS shall facilitate denial of service to all illegal communications devices within the country including SIM boxes, counterfeit, substandard, non-type approved and stolen devices.

9) The DMS has capability to isolate and deny services to the illegal devices as they have the potential of being used by those with criminal intent to compromise security.

10) It is important to note here that the system is deployed in a manner that facilitates mobile network operators to make reference to the database of all genuine devices (a whitelist) to solely verify the status of the phone device before providing service to the user. This is contrary to reports that the system will be extracting subscriber data for use by third parties.

11) All mobile operators will be required to connect to the DMS and ensure that blacklisted devices do not access mobile services. This process was initiated with the understanding of the operators through a consultative process from the conceptualization stage.

12) The system does not access subscriber personal information details, and therefore cannot access personal data as claimed in a section of the social and local media.

13) The Authority has been consulting and has engaged industry stakeholders and relevant Government Agencies in an effort to manage the proliferation of illegal mobile communications devices. The said Agencies include the Anti-Counterfeit Agency (ACA), Kenya Revenue Authority (KRA), National Police Service (NPS) and Kenya Bureau of Standards (KEBS). All mobile network operators and equipment vendors have also been engaged since the conceptualisation of the initiative.

14) I wish to note here that stakeholder engagement is a continuous process. The Authority remains committed to adhering to this constitutional requirement and will continue engaging all stakeholders on the deployment of the system.

    The Authority remains committed to its mandate of protecting the interest of ICT consumers, and the deployment of this system is indeed a clear testimony of this fact.

    Prior to deploying the system, the Authority is planning to roll out consumer awareness to increase the understanding of the scope and impact of this system to users of illegal communication devices.

    As I conclude, I wish to assure the Kenyan public that the Authority remains committed to effective regulation of the sector and protection of public interest in order to maintain confidence in the use of ICT services in the country.

Issued by:

Francis W. Wangusi
DIRECTOR GENERAL