9 June 2016

Mr. Francis W. Wangusi, MBS
Director General
Communications Authority of Kenya
PO Box 14448-00800
Nairobi

Access Now comments to the Communications Authority of Kenya, on the Draft Kenya Information and Communications Regulations 2016

About Access Now

Access Now is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world – including presence in the African Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.

Access Now advocates an approach to digital security that promotes good security policies that protect user rights, including privacy and freedom of expression. Access Now has previously commented on the establishment of the African Union Convention on Cyber Security and Personal Data Protection ("the Convention"),[1] in addition to various national and international consultations across the African Union. We now welcome the opportunity to provide feedback on the draft Kenya Information and Communications Regulations 2016 to the Communications Authority of Kenya.

Background

In 2009, the African Union came up with the Oliver Tambo Declaration whereby the AU engaged in an effort to harmonize various information and communications technology (ICT) regimes in the region, particularly around cybersecurity laws.[2]

Following the declaration, the African Union (AU) approved the African Union Convention on Cyber Security and Personal Data Protection in June 2014 at the 23rd Ordinary

---

[1] See blogs from June 2014, August 2014 and February 2015 where we have highlighted on potentially good, bad, and ugly clauses and have encouraged AU member states to attach reservations to their ratification documents, noting concerns about the specific provisions we outline in our comments: Ephraim Percy Kenyanito, 'Africa moves towards a common cyber security legal framework' (*Access Now*, 2 June 2014) <https://www.accessnow.org/blog/2014/06/02/africa-moves-towards-a-common-cyber-security-legal-framework > accessed 16 April 2016; Access Policy Team, 'African Union adopts framework on cyber security and data protection' (*Access Now*, 22 August 2014) <https://www.accessnow.org/blog/2014/08/22/african-union-adopts-framework-on-cyber-security-and-data-protection > accessed 16 April 2016; Ephraim Percy Kenyanito, 'Emerging threats in cybersecurity and data protection legislation in African Union countries' (*Access Now*, 13 February 2015) <https://www.accessnow.org/blog/2015/02/13/emerging-threats-in-cybersecurity-data-legislation-in-africa-union > accessed 16 April 2016

[2] Oliver Tambo Declaration (adopted 5 November 2009) <http://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf> accessed 16 April 2016

Session in Malabo.[3] The Convention covers a wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cybersecurity. Once in effect, the Convention requires AU states to enact personal data protection laws and develop a national cybersecurity strategy, pass cybercrime laws, and ensure that e-commerce is "exercised freely." African countries have begun to enact laws in an attempt to conform with the Convention.[4]

Subsequently, in December 2015 Kenya's Communications Authority invited the public to comment on the **draft Kenya Information and Communications Regulations 2016**, which comprised in turn of specific topic-wise draft regulations with respect to different powers conferred by the Kenya Information and Communications Act 1998 (hereinafter "KICA"). These included:

1. **Cybersecurity Regulations 2016**
2. **Electronic Transactions Regulations 2016**
3. **Broadcasting Regulations 2016**
4. **Electronic Certification and Domain name administration Regulations 2016**
5. **Infrastructure sharing Regulations 2016**
6. **Advertising Standards Body of Kenya Regulations 2016**

Passing data protection and digital security protections are critical steps to enabling greater user control over personal data, increasing protection for privacy, and securing the internet for users. We commend the Communications Authority of Kenya for consideration of its international commitments and awareness of the need to improve the security of the digital environment, particularly in Africa. However, the current draft Kenya Information and Communications Regulations 2016 contain several provisions that risk infringing human rights and chilling journalists in Kenya and beyond. We would like to take this opportunity to provide comments and suggested improvements to these proposals.

Applicable Human Rights Law

Kenya is a party to the International Covenant on Civil and Political Rights (hereinafter, the "ICCPR").[5] The ICCPR establishes certain international rights, including the right to privacy (Article 17), the right to freedom of expression (Article 19), and the right to freedom of association (Article 22). In addition, Kenya is a party to the African Charter on

[3] African Union, 'The 23rd Ordinary Session of the African Union ends in Malabo' (*African Union*, 30 June 2014) <http://summits.au.int/fr/22ndsummit/events/23rd-ordinary-session-african-union-ends-malabo> accessed 16 April 2016

[4] Ephraim Percy Kenyanito, Emerging threats in cybersecurity and data protection legislation in African Union countries' (*Access Now*, 13 February 2015) <https://www.accessnow.org/blog/2015/02/13/emerging-threats-in-cybersecurity-data-legislation-in-africa-union > accessed 16 April 2016

[5] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

Human and Peoples' Rights (Banjul Charter), which establishes the rights to dignity (Article 5) and freedom of information and expression (Article 9), among other rights.[6]

The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") provide a framework for protection of human rights against communications surveillance.[7] The Principles "apply to surveillance conducted within a State or extraterritorially" and include, Necessity, Proportionality, Transparency, Public Oversight, and Safeguards Against Illegitimate Access and Right to Effective Remedy.

Comments on specific regulations under consultation:

1. **Cybersecurity Regulations 2016**

Clause 2 (Interpretation): We find that these definitions are to a large extent derived from those in KICA and it is our view that definitions that exist in the primary legislation should not reappear in subordinate legislation.

Despite, this above fact, we find that the new definitions are confusing and we request more clarity on the whole clause on definitions - especially on the terms: communication log, computer data, content data, critical internet resource, cybercrime, cybersecurity, disruption, subscriber information, and traffic data and metadata - as there appears to be inconsistencies here with the KICA Act which need further clarification.

We further point out that the process of developing these regulations need to take into consideration that a Kenyan Cyber Bill is in development and these regulations need to take consideration of the language of the Bill that is in development to prevent contradictions.

Clause 3 (Objectives): We also request that the clause 3 (b) of the objectives ought to be deleted as these Cybersecurity Regulations 2016 are subordinate regulations and cannot most importantly create criminal offenses.

Clause 4: We find that this clause to be a duplication of KICA Act provisions s. 83U, 83X and 84B of the Act.

We request that the specific clause 4 of the regulations are reconsidered to prevent confusion.

Clause 5: We welcome the introduction of regulation 5 e) and f) as they are not covered by KICA, as they focus on data privacy. We applaud the effort of the regulator to consider data protection as outlined in Section 2 (e) and (f) of the African Union Convention on Cyber Security and Personal Data Protection. We however politely suggest that on the Kenyan Regulations a typo ought to be corrected as it states, "provided for under this **Convention."** We also urge for the fast tracking of the Kenyan Data Protection Bill to ensure safety of citizens data from data breaches.

---

[6] African (Banjul) Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M; *see also* African Union Department of Political Affairs, 'Human Righs Strategy for Africa' (14 December 2011) <http://pa.au.int/en/sites/default/files/HRSA-Final-table%20%28EN%29%5B3%5D.pdf> accessed 16 April 2016

[7] International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 16 April 2016

We also find the phrase "preliminary formalities" to be confusing at this clause and request that you define for clarity purposes.

We are also concerned that under the same clause there is a phrasing, "...the local routing of Internet traffic for purposes of effective security management…" and request for more information on the mandate is creating.

We also raise concerns that this appears to be giving an unclear mandatory data localisation mandate to Kenyan authorities (and not clear to whom amongst them). We emphasise that the government should be seeking to strengthen data security approaches that focus on users, and enacting privacy and data protection rights for them in Kenyan law - that actually meaningfully protects them and advances digital security.

We oppose mandatory data localisation measures which do not allow for transfer of data to third countries. Data should be protected at all time while stored and in transit. Mandatory data localisation undermines the fundamental openness and interoperability of the internet.

We re-emphasize that clause 5 (c) ought to be deleted as these Cybersecurity Regulations 2016 are subordinate regulations and cannot most importantly create criminal offenses and we also find clause 5 (c) to be restrictive on investigative journalists and whistleblowers. We request amendment of this to include language on exceptions for these above purposes.

Clause 6: We would like to point out that the offenses listed out in this clause are already covered in various Kenyan Laws and thus no need to create different penalties for the same offenses had they been carried out offline. These laws include the: Penal Code, Sexual Offenses Act, National Cohesion and Integration Act, Media Act No. 3 of 2007, and Films and Stage Plays Act.

Clause 7, 11, 13 (d) and 13 (e): The requirement of identification of internet users in cyber cafes is an imposition of intermediary liability on the cybercafe owners. We are concerned by this provision and request that it be amended. Otherwise, there is a great danger that this will chill freedom of speech of ordinary internet users.

We request that these clauses ought to be amended as they have broad human rights concerns. In particular, the clause on data retention is vague and dangerous as it does not state the data retention period. These clauses cannot exist as they are in the absence of a data protection law.

These clauses are also in contravention of international human rights standards for surveillance. Specifically the principle of Necessity[8] requires "[s]urveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State."

In addition, the principle of Proportionality makes the state state responsible for establishing, among others requirements, that "there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and; there is a high degree of probability that evidence of relevant and material to such a

[8] See above n 7

serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought."

In this case the Authority does not demonstrate the necessity of this data.

We also request that there is clear due process on access to the data retained (in case it is retained). This should be inline with judicial authority orders, specifically the NIS Act.

Clause 14 (a): This clause creates a dangerous proactive monitoring and reporting legal requirements on telcos and ISPs for a broad range of activities ("cyber crime"). We request that this clause be clarified to prevent imposing liability on intermediaries for them to proactively monitor cybercrime incidents. In essence, they would be forced to spy and report on their users to KE-CIRT/CC.

Clause 14 (c): We find this clause on providing information to the Communications Authority to be in contravention of Section 36 of the Prevention of Terrorism Act and Section 42 of the National Intelligence Service Act which requires that information should only be accessible after obtaining an order from the High Court.

We find the proposal by the Communications Authority to be in contravention with the principle of "competent judicial authority". The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") provide a framework for protection of human rights against communications surveillance.[9] This is the case as the regulations attempt to bypass the High Court. The principle requires, "Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate and independent from the authorities conducting Communications Surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them."

2. Electronic Transactions Regulations 2016

Clause 12: We request clarity on the term "intriguing message". We would also like to point out that this term is not mentioned anywhere in the document or other Kenyan legal documents.

Clause 14: We support the inclusion of the first part of this clause in the draft regulations and note that the second part of the clause is vague and needs stronger language to prevent intrusion into privacy rights of Kenyan users.

3. Electronic Certification and Domain name administration Regulations 2016

Clause 21 (1), (3): We request that these provisions be deleted. This is the case as limiting the trusteeship to the Communications Authority is usurping the power from the

[9] See above n 7

multistakeholder model (KENIC) through with the government of Kenya is a member of the board.

We also find (3) to be unnecessary as new sub-domains are approved by the KENIC board, which is multistakeholder and includes representation from the government of Kenya.

Clause 27: We request that the clause be amended as it would require website owners to continually adjudge the legality of comments made on their websites. This is chilling to free speech. The language as phrased requires domain name registrars to proactively policing their customer websites for content. This obligation would not be fair and would in fact create a chilling effect on free speech, since domain registrars would use their technical resources to force individual website administrators to proactively monitor and filter content - including expression that would be protected under the Kenyan Constitution and international human rights standards.

Conclusion

Improving digital security means increasing the viability and usability of the internet as a platform for communications, and its effectiveness as a driver of commerce, education, health, and development generally. Security measures are an integral to the effort to expand global access to information and communications technologies.

Access Now commends the Communications Authority of Kenya for approaching the challenging work of drafting the Kenya Information and Communications Regulations 2016. If you have any question or would like additional information, you can contact:

Ephraim Percy Kenyanito
Sub Saharan Africa Policy Analyst
Access Now
ephraim@accessnow.org

Raman Jit Singh Chima
Global Policy Director
Access Now
raman@accessnow.org