Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa

December 2016

Authors

Ephraim Percy Kenyanito, Sub-Saharan Africa Policy Analyst, Access Now
ephraim@accessnow.org
Raman Jit Singh Chima, Policy Director, Access Now raman@accessnow.org

Introduction

This policy brief examines national responses in Kenya, Ethiopia, South Africa, and Zimbabwe to the signing of the **African Union Convention on Cyber Security and Personal Data**.[1]

Specifically, we look into the following laws:

- Draft Zimbabwe Computer Crime and Cybercrime Bill
- Draft Kenyan Computer and Cyber Crimes Bill 2016
- Ethiopia Computer Crime Proclamation 2016
- Draft South African Cybercrimes and Cybersecurity Bill 2015

The briefing finds that many clauses in the bills do not follow the important guidelines created by the AU Convention. We accordingly urge all countries to ratify the Convention, which was created after multistakeholder input, before further advancing legislation that stands to harm human rights in various ways.

[1] The term "Sub-Saharan Africa" in this brief excludes the following African countries that are considered Middle East and North African countries by the International Monetary Fund: Algeria, Djibouti, Egypt, Libya, Mauritania, Morocco, Sudan, and Tunisia.

Background: the African Union Convention on Cyber Security and Personal Data

The AU Convention on Cyber Security and Personal Data improved greatly as the result of positive civil society input into the drafting process. However, the Convention has not yet entered into force and a number of countries have promulgated harmful new cybersecurity legislation after the text was finalized in June 2014.[2] Ratification requires the executive or the legislature to deposit instruments of ratification with the AU secretariat in Addis Ababa, Ethiopia. As of July 2016, eight African nations had signed the convention, including: Benin, Chad, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia.[3] Senegal ratified the convention in the July-November period, and remains the first and only country to have done so.[4]

However, the lack of ratification has not stopped several countries from racing ahead with rushed, and potentially harmful, legislation. After surveying 45 Sub-Saharan African countries, a total of 13 countries have attempted domestic reforms of ICT laws in the period between June 2014 and September 2016, including Benin, Botswana, Chad, Ethiopia, Kenya, Madagascar, Namibia, Nigeria, South Africa, Tanzania, Uganda, and Zimbabwe.

Several of the domestic reform bills fail to provide basic protections for user data.[5] Worse, other bills enable the government to violate the rights of privacy, expression, and assembly. In our view, some of these errors stem from overbroad interpretation of the ITU Harmonization of the Telecommunication and ICT Policies and Regulation in Africa (HIPSSA) project, which was carried out prior to 2014 without public consultation.[6] Unlike the ITU model regulations, this Convention was adopted after multistakeholder input, with the African Charter on Human and People's Rights as a reference. For this reason,

---

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

[3] <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S5P3_Souhila_Amazouz.pdf> accessed 20 August 2016.

[4] Dr Papa Assange Touré, 'A decisive step by Senegal towards accession to and ratification of the Budapest and Malabo Conventions' (*Observatoire-FIC.com*, 2 May 2016) <https://www.observatoire-fic.com/a-decisive-step-by-senegal-towards-accession-to-and-ratification-of-the-budapest-and-malabo-conventions/> accessed 22 October 2016
(Senegal ratified the convention in the July-November period after the Senegal council of 30 March 2016 adopted bills authorising the President of the Republic of Senegal to ratify the African Union Convention on Cyber Security and Protection of Personal Data of 27 June 2014, and the Budapest Convention on Cybercrime of 23 November 2001 and its additional protocol of 28 January 2013 concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems)

[5] Cyber Security Models And Initiatives In Selected African Countries' (*oAfrica*, 2012) <http://www.oafrica.com/ict-policy/cyber-security-models-and-initiatives-in-selected-african-countries/> accessed 15 August 2016.

[6] in 2008 the Ministers in charge of Communication and Information Technologies from the African Union countries adopted a Reference Framework for Harmonization of the telecommunication and ICT Policies and Regulation in Africa (HIPSSA) (Cairo, 2008) during the 2nd Conference of African Ministers in charge of Communication and Information Technologies (CITMC-2). The Reference Framework adopted had one of the key aim, to: *"...Establish harmonized policy, legal and regulatory frameworks at the regional and continental levels to create an enabling environment that will attract investment and foster the sustainable development of competitive African Telecommunication/ICT regional markets, infrastructures, and to increase access [of its people to the related services..."* We can highlight that the International Telecommunication Union supported this initiative under the HIPSSA with a focus on key economic integration organizations in Sub-Saharan Africa <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx> accessed 15 August 2016.

governments should not pass the suggested ITU regulations into law, but should follow the AU Convention instead.

But before countries further codify harmful laws, Access Now urges them to first ratify the AU Convention. Once they have done so, they should carefully implement the Convention's framework with legislation that respects human rights. These domestic reform efforts should be carried out in open, consultative, multistakeholder processes with input from civil society organizations and subject-matter experts.

Applicable Human Rights Law and Norms

Kenya, Ethiopia, South Africa and Zimbabwe are parties to the International Covenant on Civil and Political Rights (the "ICCPR").[7] 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, these countries are parties to the African Charter on 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.[8]

The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") provide a framework for the protection of human rights against communications surveillance.[9] 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.

Positive Protections

- **Protections for security researchers**

The draft Computer and Cyber Crimes Bill 2016 contains clauses which allow for the protection for digital security researchers if they find and demonstrate the existence and extent of systems vulnerabilities. Sections 4 (2), 6 (2) and 8 (3)(a) protect digital security researchers as they find and demonstrate the existence and extent of systems vulnerabilities. This is a model provision for other cyber drafts in the region.

- **Protections against intermediary liability**

We found that across Kenya, Ethiopia, South Africa and Zimbabwe draft laws, there are clear provisions protecting intermediaries from liability for hosting third party content.[10] This type of legal protection enabled the growth of the internet and allows the smooth functioning of the global web at scale, so these provisions must be retained.

---

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

[8] 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 November 2015

[9] International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 16 November 2015

[10] Section 30 of Kenyan draft law, Section 34 and 39 of Zimbabwe draft law, Article 16 (3) of Ethiopian law, Section 64 of South African draft law

Issues of Concern

- **Restrictions on whistleblowers and digital security researchers**

Ethiopia, Zimbabwe, and Kenya's draft laws contain sections on "computer fraud" and "illegal access." These provisions are vague and could be interpreted to criminalize the work of journalists, whistleblowers, and digital security researchers

- **Ethiopia: Article 10 of its 2016 Computer Crime Proclamation** focuses on computer-related fraud and can be harmful to journalists because the clause does not define the meaning of "distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal." The vague language leaves open the possibility of potentially misuse of Article 10 in the course of prosecution or for state authorities to use the article to pressure journalists to reveal journalistic sources or to prosecute anonymous or pseudonymous activity online.

- **South Africa**: **Section 4 of the Cybercrimes and Cybersecurity Bill 2015** makes it an offense for a person to gain "unlawful and intentional access to the whole or any part of" data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure. For the section, "access" includes, to "make use of," "view," or communicate with," among other actions. A person's actions are unlawful to the extent that they exceed lawful authority to access.[11] This circular definition fails to offer guidance as to when access to such systems exceeds an individual's lawful authority.

- **Vague provisions and criminal defamation provisions which are open to abuse**

Across all four jurisdictions, we found vague sections which added additional fines and jail time when offenses are stacked.[12] The most dangerous clause is in the Ethiopian text, which aims to punish whoever causes "conflict among people." This provides no clear evidentiary standard to provide notice as to what behavior is proscribed -- a requirement for any law to meet international human rights standards.

We recommend to the Ethiopian government that it consider the ruling by the African Court on Human and Peoples' Rights (African Court) in the *Lohé Issa Konaté v. Burkina Faso* case, in which the Court called for the repealing of criminal libel laws. Ethiopia should also consider General Comment No. 34 of the Human Rights Committee, the UN body which officially interprets the ICCPR, which recommends that state parties to the ICCPR "consider the decriminalization of defamation" and recommends that, in any case of defamation, "imprisonment is never an appropriate penalty."[13]

[11] Sections 4 through 10 similarly create offenses for unlawful activities. Protections for security research, whistleblowing, and journalism should similarly be addressed.
[12] Section 5, 13, 33 of Kenyan draft law, Section 15 and 41 of Zimbabwe draft law, Article 2, 9, 13. 14, 23 of Ethiopian law, Section 38 of South African draft law
[13] UN Human Rights Committee (HRC), *General comment no. 34, Article 19, Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34 , available at: http://www.refworld.org/docid/4ed34b562.html [accessed 26 August 2016]

- **Criminalization of computer use**

Across Kenya, Ethiopia, South Africa, and Zimbabwe draft laws we found sections adding penalties and imprisonment terms for any person who commits an offense under any other law, through the use of a computer system.[14] We recommend that these sections be removed as the offenses listed are already covered in existing laws in the respective countries. Redundant provisions adding penalties for using a computer do not achieve legitimate public policy goals, and can slow the adoption of new technologies.

- **Mandatory data retention provisions**

In Kenya, Zimbabwe, and Ethiopia, the relevant texts contain vague provisions on data retention; they do not state the maximum data retention period.[15] This is a dangerous trend because data can be retained forever, allowing for data breaches and creating a burden on the entity preserving the data. These draft provisions contain language on mandatory data retention despite the absence of data protection laws.

We recommend removing these provisions, as they are harmful for human rights, increase digital security risks, and are often counter-productive. Rather, we recommend that governments powers to issue data retention orders should be limited to specific cases and individuals, subject to court warrants and other oversight.

We further recommend that governments review the judgment of the Court of Justice of the European Union in Joined Cases C-293/12 and C-594/12,[16] where the court struck down similar data retention provisions. They should also consider the EU Data Retention Directive, which found a "*serious interference with the enjoyment of the fundamental rights*" and that "*it was...vague...and..would interfere with the entire populations.*"[17]

Any request for data to be retained must only be via warrants issued by courts. We find no recourse for citizens in case of a breach of this retained data. As per the International Principles on the Application of Human Rights to Communications Surveillance, the principle of Integrity of Communications Systems states that:

> *States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.*

In the case that data are necessary, we recommend the amendment of these sections to require that when a warrant is issued for particular data to be retained, that there be a maximum period of retention of the data.

- **Illegally obtained evidence and government hacking**

In Ethiopia, Zimbabwe, and Kenya,[18] we found provisions which can be interpreted to allow government hacking. Particularly, we found that the drafts were vague and lacked

[14] Section 19 (1) of Kenyan draft law, Section 20 and 40 of Zimbabwe draft law, Article 19 and 20 of Ethiopian law, Section 66 of South African draft law
[15] Section 33 (2) of Kenyan draft law, Section 31 and 32 of Zimbabwe draft law, Article 24, 31, and 33 of Ethiopian law,
[16] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322> accessed 16 August 2016
[17] See above n16
[18] Article 32 (2)- 2 and 33 Ethiopia Computer Crime Proclamation 2016, Section 33- (1) and Section 36 (1) Draft Zimbabwe Computer Crime and Cybercrime and Section 20 (2), Section 21 (4), Section 26, Section 27 and Section 36 (a)Draft Kenyan Computer and Cyber Crimes Bill 2016.

judicial and legislative oversight, and that the current language does not compel law enforcement to return devices upon completion of investigations.

The practice of "government hacking" significantly interferes with human rights, such as the right to privacy, as well as threatening personal property rights and global cybersecurity. We recommend that amendments are made to prohibit the use of government hacking operations to access data stored remotely. Particularly the laws should conform to Access Now policy brief, "A Human Rights Response to Government Hacking," requiring that:

> *Government hacking must be provided for by law, which is both clearly written and publicly available and which specifies the narrow circumstances in which it could be authorized. Government hacking must never occur with either a discriminatory purpose or effect.*[19]

- **Lack of competent judicial authority and due process**

In Kenya, Zimbabwe and Ethiopia, we found provisions which would bypass the judiciary because police officers are not required to apply for a court warrant while investigating cybercrimes.[20]

We recommend that these sections be amended as they contravene the principle of "competent judicial authority" in the International Principles on the Application of Human Rights to Communications Surveillance.[21] The amendments should require that cybercrime be investigated under the supervision of competent judicial authorities.

- **Lack of user notification, transparency, and due process**

The Ethiopian, South African and Zimbabwean draft laws do not have provisions for user notification and transparency.[22] However, under Kenya's draft Computer and Cyber Crimes Bill 2016, attempts to provide for an appeal mechanism under Section 29 for anyone aggrieved with decisions of the High Court regarding offenses under this law. However, we believe that there is a general lack of clear procedures regarding user notification as to communications surveillance.

We recommend that the draft laws require law enforcement to publish records of requests for communications surveillance, and clarify that service providers have the authority to publish such records.

Looking Ahead

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,

---

[19] <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf> accessed 25 November 2016

[20] Section 21 (1), 24 (6) and 35 (2) of Kenyan draft law, Section 33- (1) and Section 36 (1) of Zimbabwe draft law, Article 32 (2)- 2 of Ethiopian law,

[21] See above n9

[22] The principle of Transparency says that the state "should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each." Further, "States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance. See above n5

health, and development generally. Security measures are integral to the effort to expand global access to information and communications technologies.

We recommend that national authorities fulfill their obligations under the African Charter on Human and People's Rights and other international on human rights treaties, and should ensure that they involve the multistakeholder community in policymaking processes.

Access Now *(accessnow.org) defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.*