CIPESA ICT Policy Briefing Series
February 2015

Reflections on Uganda's Draft Data Protection and Privacy Bill, 2014

Background

The respect for privacy and protection of users' data is an ongoing concern, both in the online and offline spheres. Whereas the privacy of individuals generally and sometimes of their communications is guaranteed by national constitutions in several African countries, the absence of privacy and data protection laws has led to increased calls for enactment of laws that safeguard online users' privacy and data.[1]

Of the five countries that constitute the East African Community (EAC) – Burundi, Kenya, Rwanda, Tanzania and Uganda - none has a data protection and privacy law. There are some relevant provisions in other legislations, including laws governing telecommunications and electronic services. However, these are non-exhaustive. Moreover, there are claw back clauses in laws on security, interception of communications, terrorism, and telecommunications services provision, among others.

In March 2014, the Tanzanian Minister for Communications, Science and Technology announced government's plan to adopt a Data Protection Act by the end of 2014.[2] Similarly, in Kenya a Data Protection Bill, 2013 was tabled in Parliament in 2014 but it has hardly progressed since then.

Towards the end of 2014, Uganda's government through the National Information Technology Authority (NITA-U), Ministry of Information Communication and Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MOJCA) issued a draft Data Protection and Privacy Bill for public comment. The Bill seeks to protect the privacy of the individual and personal data by regulating the collection and processing of personal information. It provides for the rights of persons whose data is collected and the obligations of data collectors and data processors; and regulates the use or disclosure of personal information.

The drafting of the Bill comes at a time when more Ugandans are getting online. The Uganda Communications Commission reports 53% mobile phone penetration and 23% internet access rates among the country's population of 39 million. While the move by government to develop this Bill reflects its appreciation of the need for safety and security of citizens online, the proposals should be studied keenly to ensure that the protections offered by the bill are adequate.

In this brief, we interrogate some of the problematic clauses in the Bill that require further consideration by the drafters.

Open to misinterpretation

Some of the wording of the Bill should be clearly defined for a consistent understanding of their application and avoidance of misinterpretation. Broad terminology is used in Section 4(2), which states that personal data may be collected or processed where the collection or processing is necessary (i) for

[1] State of Internet Freedoms in East Africa, 2014, An Investigation Into the Policies and Practices Defining Internet Freedom in East Africa, An OpenNet Africa Report, http://www.cipesa.org/?wpfb_dl=76
[2] Tanzania: Data protection bill announced as part of cybersecurity, initiativeshttp://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2415

the **proper performance** of a **public duty** by a public body and for (ii) **national security.** The phrases, *"proper performance", "public duty" and "national security*" require specific qualification as they are open to abuse due to their broad definitions. Unspecified matters of "national security" also permit the collection of data directly from a data subject in Section 7, thus leaving citizens' information open to unwarranted access.

Section 6 states that a "data controller or data processor or person collecting or processing personal data shall collect or process the data in a manner which does not infringe the privacy of the person to whom the data relates." There needs to be a clear definition of what constitutes "**privacy infringement**" as lack thereof leaves users' data open to abuse by data collectors and processors.

Similarly, the type and amount of data that can be requested and stored is also open to various interpretations. Section 10 (1) states that a data collector or data processor shall only process the **necessary** or **relevant personal data.** However, there is no indication of what can be defined as "necessary" or "relevant". Sub-section (2) tries to address this by stating that data processed should not be "in excess of the data which is authorized by law or required for a specific purpose." The Bill, however, lacks a clause which defines what can be considered "**excess data**."

In its current form, the Bill allows widespread collection and processing of personal data, placing restrictions only on data related to "religious or philosophical beliefs, political opinion, health or sexual life" (Section 5(10)). As currently formulated, even this clause leaves room for collection and processing of data outside of these restrictions.

Unclear Extent of Privacy Protections and Security

Although Section 7 (2) (g) states that "data can be collected from another person, source or public body where it is not **reasonably practicable** to obtain the consent of the data subject," depending on the circumstances under which the information is required, data could be provided by other sources without the owner's consent under the guise of it not being 'reasonably practical' to obtain the data subject's consent. The circumstances under which this could happen need to be specified to ensure the protection of data in the absence of consent.

Further, the length of time that collected personal data can be retained is not indicated and raises concern about the legitimate use of citizens' data. While Section 14(1)(3) states that data cannot be held for a **period longer than is necessary**, the actual period is not indicated. We therefore recommend that the data retention period be clearly indicated in the Bill. The retention of data for **national security** purposes also raises concern for the security and use of personal data as, yet again, national security is not defined.

Transparency is infused into the Bill as seen in Section 9 (1), which calls for a data subject to receive notification prior to data collection, including the nature of data being collected, the purpose for which the data is required, indication of whether or not the data required is discretionary or mandatory, the right to access the data and the right to request rectification of data. However, there is no notification provision for the security measures in place for safeguarding the data due to be collected. A clause that indicates the guarantee of the security of data provided should be included.

In Section 15, it is not clear what happens when a data controller does not provide security measures for data stored, while Section 17 does not state what happens when a data controller discloses data unlawfully. Penalties for defaulters need to be clearly stated.

Further in Section 18, on 'notification of data security breaches', rather than simply stating that the data subject should be notified "immediately", the Bill should specify a timeframe within which a data controller should notify a data subject after getting knowledge of the breach. We recommend a maximum notification time of two working days. This notification should, wherever applicable, be done through multiple communication channels as per the contact details provided by the data subject. Besides, publishing of a breach on the website or in mass media may further put the privacy and data of a data subject at risk and potentially lead to further breaches to the privacy of the data subject. The mass media measures proposed in the Bill should not be employed if any details about the particulars of the affected individual or of the nature of breaches are to be communicated. Instead, telephonic notification may be added to email and to last known residential or post address.

While Section 23 tries to enforce protection of data, it fails to clearly state the penalties that data controllers should face for contravening the law. It also does not mention the actions which would constitute failure to protect data and privacy such as negligence and unauthorised access and dissemination.

Further, the Bill does not address protection of data collected by data processors or controllers operating beyond Uganda's borders but utilising data belonging to Ugandan individuals or organisations. We recommend that a principle on jurisdiction be added in the Bill and penalties indicated for any defaulters. The proposed clause should read as follows: *"Personal data shall not be transferred to a country or territory outside Uganda unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

Access to Personal Information

Although Section 19 grants data subjects access to their personal information that has been collected, upon submission of a request in a **"prescribed manner"** and proof of identity, there needs to be clarity on what constitutes the **"prescribed manner"** through which to make requests. In regard to the data requesters paying a **"prescribed fee"** as a requirement to receive information, this fee should be nominal (UGX 1,000) to facilitate even access for citizens with limited financial means. In instances where requests are made using electronic means such as email, we suggest that requesters are exempted from making any payments at all.

We further suggest that the Bill under **Section 19 (9) i**ndicates a prompt timeline within which a data subject must receive a response from the data controller. The suggested **30 days** for a data controller to comply with a request are too many and should be reduced to no more than 10 working days.

Besides, the format in which data is held plays a role in how it can be received by a requester and as such there should be a clear indication of the prescribed format in which data should be disclosed to a data subject.

Section 26 indicates that that the public shall have access to information held by the Data Protection Register, which is a record of "every person, institution or public body collecting or processing personal data." However, it does not define the mechanisms of access to the Register - whether access is free, electronic or physical. We thus recommend that the Bill clearly states the access mechanisms to the 'Register'.

Further processing

The use of data for unsolicited marketing has for a long time been debated globally and in Uganda. Although the Bill seeks to address this under Sections 20 and 21 by allowing a data subject to write to a data controller to request an end to processing of personal data including for the purposes of direct marketing, the 14 days provided for notification of compliance, notification of intent or non-compliance to prevent processing of personal data are very long, as within that period further processing could potentially be ongoing. A clause for suspension of further processing within 48 hours of receipt of a request should be added, with the 14 days being the timeline applied thereafter for notice of compliance, intent or non-compliance to requests against further processing.

Also the mechanisms for obtaining consent from the data subject for further processing should be indicated in the Bill.

Penalties

In regard to the proposed penalties on unlawful disclosure and sale of personal data, we believe that the fine of **120** currency points or five year imprisonment or both is financially lenient for offenders. We therefore propose for an increment in currency points to **1000**.

We further suggest a clause that specifies the penalty for a data processor/ controller who through omission (such as negligence) or commission fails to secure a data subject's data, leading to its falling into unauthorised hands. Offenders should face similar penalties as proposed above.

Continuous stakeholder engagement

The Uganda Data Protection and Privacy Bill drafting phase should engage with and seek consultations with different stakeholders including civil society, private sector, government and academia for an extended period prior to tabling before parliament. This will ensure that the Bill, before being passed into law, is inclusive, accommodative and addresses the concerns raised by all stakeholders.

CIPESA's formal submission on the Data Protection and Privacy Bill 2014 can be accessed here.