THE CENTER FOR POLICY ANALYSIS (CEPA)

Home of Parliament Watch Uganda

DATA PROTECTION IN THE DIGITAL AGE: AN ANALYSIS OF UGANDA'S DATA PROTECTION AND PRIVACY BILL, 2015.

POLICY SERIES PAPERS NUMBER 19 OF 2018

Published by CEPA

P. O. Box 23276, Kampala
Email: info@cepa.or.ug
Web site: http://www.parliamentwatch.ug
www.cepa.or.ug

By Irene Ikomu

Citation
Ikomu I, (2018). Data Protection in the Digital Age: An Analysis of Uganda's Data Protection and Privacy Bill 2015. CEPA Policy Series Papers Number 19 of 2018. Kampala

With inputs from

Isaac Okello
Jacky Kemigisa
Eshban Kwesiga

Abstract

While Article 27 of Uganda's constitution provides for citizens' right to privacy, there is no law to protect an individual's data privacy despite the large amounts of citizen data collected by government departments and private entities on a regular basis. New rules passed by the Uganda Communications Commission to streamline citizen bio data are well intended but there are concerns about how feasible the implementation is. More concerning, is that this data is collected with no guarantee of its protection and privacy. Existing legislation prohibit unauthorised access and disclosure of information. Current laws include; the Access to Information Act 2005, Uganda Communications Act, 2013, Electronic Signatures Act 2011, Computer Misuse Act 2011, and the Regulation of Interception of Communication Act 2010. However, the provisions in these laws are not elaborate and do not adequately protect personal data.

According to the Uganda Internet Usage and Telecommunications Report, Uganda's Internet subscribers have increased spontaneously in the past two years, in 2010 the Internet subscribers increased by 9.6% and in 2016 and 2017, the growth was over 30%, which is very impressive. Uganda has 2.2 million active Facebook subscribers. In absence of a comprehensive law and in light of the Cambridge Analytica scandal where the UK firm harvested data from millions of Facebook users to predict and influence the behavior of voters, a Bill to protect citizen data is a welcome step forward. However, vague wording has left the Bill open to misinterpretation, unclear procedural processes for collection and retention, as well as the costs associated with accessing personal data. Care should be taken to balance civil liberties, national security and data protection and privacy.

This policy paper will review the opportunities and gaps within the provisions of the Data Protection and Privacy Bill and whether it will effectively protect citizen's data.

Introduction

Background to the Bill

As the world continues to become more digitally connected, public and private business models are generating more and more personal data and processing that data in different ways. In Uganda, Internet users have increased in the past two years; in 2010, Internet users increased by 9.6% and in 2016 and 2017, the growth was over 30% to a little over 13,000,000 (thirteen million) Internet users at the end of 2017.[1] For many of these Internet users, their data is being collected, networked and correlated everywhere- on social networking sites, new digital businesses and websites cropping up every day. Similarly, government agencies, telecom companies and new technology-driven businesses like Safe Boda and Uber are all collecting, analysing and using this data in various ways and for different purposes.

The protection of data has been the subject of ongoing conversations globally. As more businesses transform digitally, how they handle and analyse data is coming under intense scrutiny. A good example is the recent investigations into Facebook in the USA, UK and

[1] Uganda Internet Usage and Telecommunications Report, 2017

European Union, given the data breach scandal involving Cambridge Analytica- a British consultancy firm that harvested and misused data from 50 million members.[2] With advancements in technology, increased cross-border trade and the with cybercrime growing by the day, businesses and governments are prioritising data protection and data privacy to avoid financial loss and maintain steady productivity.[3]

Uganda does not currently have a law that effectively regulates the collection and storage of data by 3rd parties. The protection of citizen data must achieve a balance between giving people more control over their personal data and allowing data vital for our economy, our democracy and our protection to be processed without interruption. In this regard, Uganda is not the only country debating what appropriate legislation should look like. As more and more users, businesses and public processes get online, it is now more important than ever to set up these protections.

There are only 17 countries in Africa that have enacted comprehensive personal data protection laws; Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara[4]. The African Union (AU) adopted the AU Convention on Cyber Security and Data Protection (AU Convention) in June 2014.[5] However, the AU Convention has not currently taken effect as it has, to date, not been ratified by 15 out of the 54 AU member states. Nonetheless, the AU Convention provides a personal data protection framework which African countries may potentially transpose into their national legislation, and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data, taking global digitalisation and trade into account.

The European Union (EU) currently has the most comprehensive laws regulating data protection and privacy.[6] The EU passed the General Data Protection Regulation (GDPR) to harmonise all data protection laws across all countries in the EU, by giving all citizens better control over their personal data and simplifying the regulatory environment for international businesses. The new regulation replaces the EU's 20-year-old data protection directive, which was created when just one percent of Europeans were online. It allows citizens to request to see what data companies have about them. EU citizens can also request to modify that data if it's incorrect, or delete that data, or even export it.

---

2 Facebook Rocked by Data Breach Scandal, https://www.nation.co.ke/news/world/Probe-on-Facebook-data-leak-looms/1068-4349168-nhprupz/index.html, accessed on 19/0718

3 Privacy is Paramount: Personal Data Protection in Africa, Deloitte, 2017 p.3

4 Cynthia Rich (2016) Privacy Laws in Africa and the Near East (16) 6 Bloomberg BNA World Data Protection Report, 1

5 Ibid

6 The European Union (EU) General Data Protection Regulation (GDPR) officially came into force on 25 May 2018

Existing Legal Framework

While Article 27 of Uganda's constitution provides for citizens' right to privacy, there is currently no law to protect the privacy of an individual's data despite the large amounts of citizen data collected by government departments and private entities on a regular basis. New rules passed by the Uganda Communications Commission to streamline citizen biodata are well intended but there are concerns about how feasible the implementation is. More concerning, is that citizen data is currently collected with no guarantee of its protection and privacy.

Existing laws including the Access to Information Act (2005), Uganda Communications Act (2013), Electronic Signatures Act (2011), Computer Misuse Act (2011), and the Regulation of Interception of Communication Act (2010), do not effectively cover aspects related to unauthorised access and disclosure of information. The provisions in these laws are also not elaborate and do not adequately protect personal data that is collected. In absence of a comprehensive law, more concrete legislation to protect citizen data would be a welcome step forward.

A Justification for the Bill and Salient Features

According to the draft Bill, the object of the legislation is to protect the privacy of individuals and of personal data by regulating the collection and processing of data.[7] The Bill also seeks to provide for the rights of persons whose data is collected and the obligations of data collectors, data processors and data controllers as well as to regulate the use of or disclosure of personal data.

The Bill defines personal data as any information about a person from which the person can be identified that is recorded in any form[8] and includes the following qualifiers

a) Data that relates to the nationality, age or marital status of a person
b) Data that relates to the educational level, or occupation of the person or data that relates to a financial transaction in which the person has been involved
c) An identification number, symbol or other particulars assigned to the person and
d) Identity data

This Bill intends to apply to not only written and electronic records in the public and private sectors, but also covers personal data of individuals as well. In the digital age, in order to give individuals more control over their data, the law must allow them to:

- have the right to be forgotten and ask for their personal data to be erased
- ask social media to delete information they posted in their childhood
- end reliance on default opt-out and pre-selected tick boxes

---

7 Bill. No. 32 Data Protection and Privacy Bill, 2015

8 Ibid p.4

It should also:

- introduce safeguards to prevent and detect fraud, protect the freedom of the press, allow scientific research and maintain the integrity of professional sports
- include specific measures to allow action against terrorist financing, money laundering and child abuse
- allow processing done for legitimate interests so long as it achieves a balance with individuals' rights

Aside from the preliminary section, Uganda's Data Protection and Privacy Bill is divided into 7 parts; principles of data protection, data collection and processing, security of data, rights of data subjects, data protection registry, complaints and offences.

a) Principles of data protection

This section lists seven key principles of data protection that a data collector and controller is expected to adhere to when collecting, controlling and using data. In summary, the principles in many ways mirror the OECD Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data[9] and call for accountable collection, fairness, time restrictions.These principles are minimum standards to abide by and therefore must be spelt out comprehensively hence the following recommendations:

Clause 3 (1) (b) and 3 (1) (f) should be merged amended to read as follows: collect and process data fairly, transparently and lawfully with the participation of the data subject in the collection, processing and holding of the personal data

Clause 3 (1) (c) and 3 (1) (e) should be merged and amended for better clarity as follows: collect, process, use or hold adequate, relevant personal data as well as ensure quality of information collected, processed, used or held; and where necessary, keep data up to date with inaccuracies rectified without delay.

Clause 8, which provides that data should only be collected for a specific and lawful purpose, should be moved from Part III of the Bill to this section to fit within the principles under clause 3.

Clause 3 (1) (g) should be amended for better clarity as follows: observe security safeguards in respect of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate measures.

b) Data collection and processing

This part of the Bill focuses on regulating how data is collected and processed and runs from clause 4-Clause 15 of the Bill. These clauses cover: consent to data collection, limits of collecting and processing data, protection of privacy, the collection of data including

[9] http://www.oecd.org/sti/ieconomy/49710223.pdf

quality and timeframe, correction of personal data, retention of records and processing data outside Uganda.

The biggest concern under this section is with consent. Clause 4 (1) provides that a person shall not collect or process personal data without the prior consent of the data subject. Unfortunately, the Bill does not define what consent means or how consent should be obtained from persons whose data is being collected. These need to be properly elaborated in the Bill. Further, the definition of consent must also include the right to object or to withdraw consent as well as a requirement to inform the data subject how the data will be used including disclosing the existence of automated decision-making.

This section of the Bill also needs to include the kind of safeguards anyone collecting data needs to put in place to protect sensitive personal data. The EU's GDPR, for example, requires all data collectors to set up security safeguards to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage, against data collected using appropriate measures.

A final point under this section is with regard to processing personal data outside Uganda.[10] This is especially relevant in relation to multinational organisations with large global footprints that transfer personal data across borders in the ordinary course of business; such as businesses that use cloud technology and cloud-based solutions that seek to make data instantly available across the world. Clause 15 currently only requires such a data processor to ensure that the country where this data is finally held has adequate data protection measures in place. By comparison, South Africa requires additional safeguards including the need for binding corporate rules that provide adequate protection, an agreement between the sender and receiver that provides adequate protection, and the data subject's consent to the cross-border transfer.[11] Uganda's Parliament, therefore, needs to debate a balance that increases safeguards for personal data and privacy without curtailing international trade as there is already a concern over the differences in legislation across the continent and how that might affect businesses.[12]

c) Security of data

Clauses 16-19 of the Bill cover security of data including the general scope of security measures including in relation to data processed by the data processor, data processed by an authorized person and notification of data security breaches.

There are two points of concern within this section. Firstly, while the Bill defines who a data processor is, it does not define what/who a data operator is as provided for under

---

10 Clause 15, Data Protection and Privacy Bill 2015

11 S. 72, The Protection of Personal Information Act, Republic of South Africa

12 Deloitte, *supra* p.7

Clause 18 of the Bill. This definition should be included in the definition section of the Bill.

Secondly, clause 19 provides that in case of data breach, the data collector/processor/controller "shall immediately notify the authority…." And does not include a provision for notification of the data subject in case of a breach. An individual has the right to be notified in case of any breach of their personal data as it amounts to a violation of the person's privacy protected by Uganda's Constitution.[13] The law should include a timeframe within which the person whose data has been breached is notified. It should not be left to the authority to determine whether a person should be notified in case their data is breached as it currently provides in Clause 19 (3).

d) Rights of data subjects

The rights of data subjects are provided for under clauses 20-24 and include the rights to access personal information, prevent processing of personal data, prevent processing of personal data for direct marketing, as well as rights in relation to automated decision-making and rectification, erasure and destruction of personal data.

Automated decision-making is the ability to make decisions without human involvement and involves special categories of data such as information about health, sexuality and religious beliefs; while profiling is a form of automated processing of personal data used to analyse or predict matters relating to an individual,[14]for example analyzing a person's interests to tailor ads. If these are not properly regulated, they leave room for gross violations of privacy.

Unlike the Bill that requires notice to the data subject where a decision that affects a subject is based solely on automated processing, the EU's GDPR expressly prohibits decisions based solely on automated decision making which produce legal effects except where it is necessary for executing a contract, where it is authorized by law or where it is based on the data subject's explicit consent.[15] In Uganda's case, necessity should be interpreted narrowly, and the clause needs to be reworded so that organisations must tell individuals when a decision has been taken solely using automated decision-making and be able to show that it is not possible to use less intrusive means to achieve the same goal.

It would also be prudent to expand the scope of information that a data subject has access to beyond just a 'description of personal data' as currently provided for under clause 20 (1) (b). It should be expanded to also include other aspects of the information such as what that data is used for by the data controller. The data should also be made available in accessible formats for all people interested in their data.

---

[13] Article 27 (2), Constitution of the Republic of Uganda

[14]

[15] Article 22 (1) GDPR

The right to prevent the processing of personal data provided for under clause 21 should also be expanded to include minimum requirements for processing data such as the absolute right to withdraw consent by an individual without having to first demonstrate unwarranted substantial damage or distress as a result of the processing.

Clause 24 provides that a data subject may by notice in writing require a data controller require to ensure that any decision taken by or on be held of the data controller is not based solely on the processing by automatic means of personal data. This provision is problematic on two levels. Firstly, it puts the burden on the data subject to write to the data controller whereas the burden should be on the controller. Secondly, it does not provide for the regulation of profiling.

e) Data protection registry

Clauses 25 and 26 provide for a data protection registry, which includes the procedure for lodging complaints of breach, the authority's power to investigate, compensation for breaches and the process for appeals.

The Bill proposes the National Information and Technology Authority (NITA-U) as the supervisory authority. NITA is a parastatal that was established under the NITA-U Act in 2009. It is generally overseen by the Minister of ICT and National Guidance and provides technical support and expert guidance to government on matters concerning advice on the establishment of e-government, enforcing standards, information management and promotion of access to ICT by special interest groups.

Enforcement is key to ensuring compliance. An effective independent authority should have the powers to investigate, inspect and impose fines, which NITA-U currentlydoes not possess, nor does the current Bill provide for such powers. Both the Bill and the NITA-U Act would, therefore, need to be amended. The law properly provides for complaints and offences under the Bill including unlawful obtaining and disclosure of personal data, the sale of personal data, and offences by corporations that include failure to comply with the law. Proper enforcement is absolutely necessary for proper implementation of this law and Parliament must ensure that if indeed NITA-U should take on this role, it is properly equipped to enforce it.

Conclusion

The introduction of this Bill is a good step towards better protection for data and privacy of Ugandans. In order to effectively achieve data protection and privacy, the Bill should align with universal mechanisms including the African Union guidelines.

The Bill also needs to be thoroughly reviewed to eliminate ambiguity and ensure the right to privacy is not abused in any way through this legislation while also finding a way to balance the personal and business interests of Ugandans with the government's intentions not compromise on national security.