Privacy in Uganda

An Overview of How ICT Policies Infringe on Online Privacy and Data Protection

CIPESA ICT Policy Briefing Series No. 06/15
December 2015

CIPESA

Introduction

As of June 2015, Uganda had an internet penetration rate of 37% and there were 64 telephone connections per 100 inhabitants.[1] This was made possible by increasing investments in the Information Communication Technologies (ICT) sector by the private sector and – to a lesser extent - the government, proliferation of affordable smart phones and a steady decrease in internet costs enabled by a liberal competitive telecommunication sector.

Through the national backbone infrastructure project, government has laid a total of 1,400 kms of fibre optic cable connecting major towns and government agencies across the country.[2] Uganda is a landlocked country but its telecom and internet service providers are connected to high-speed submarine cables landing at the East African coast through Kenya and Tanzania. These cables include the East African Submarine cable System (EASSY), The East African Marine System (TEAMS), and SEACOM.

A universal access fund known as the Rural Communications Development Fund (RCDF), which is funded by a 2% levy on telecom operators' revenue, has supported the establishment of internet points of presence (POPs), internet cafes and ICT training centres, among other internet related infrastructure across the country.[3]

Uganda is experiencing a decline in internet access costs. In 2012, the daily cost of mobile browsing for 20MB of data was UGX 500 (US$ 0.14) while a limited monthly mobile bundle for 1GB cost UGX 30,000-49,000 (US$ 9 – 14).[4] As of November 2015, average daily cost for mobile browsing for 10MB is UGX 300 while 1GB costs between UGX 28,000 (US$ 8) on Uganda Telecom[5] and UGX 35,000(US$ 10) on the MTN Uganda and Airtel Uganda.

With new market entrants, the internet market is competitive with speeds being a key customer choice determinant. Also, many internet service providers (ISPs) provide free access to some features of social networks such as Facebook.[6]

In 2014, 6.7 million Ugandans were reported to be living below the poverty line compared to 7.5 million in 2010.[7] Average income per capita is US$ 680.[8]

1 UCC, "Status of Uganda's Communications Sector," October 2015, http://ucc.co.ug/files/downloads/Annual%20Market%20Industry%20Report%202014-15-%20October%2019-2015.pdf

2 "NBI/EGI Project," National Information Technology Authority – Uganda, accessed March 16, 2015, http://www.nita.go.ug/projects/nbiegi-project.

3 See the latest RCDF annual report here: http://ucc.co.ug/files/downloads/RCDF%20Annual%20Report%202014-15.pdf

4 UCC (2012), Mobile Internet Explained; http://www.ucc.co.ug/files/downloads/Mobile%20Broadband%20FAQs%20and%20Prices%20Final%20Final.pdf

5 Uganda Telecom, Mobile Data Bundle, http://www.utl.co.ug/internet/data-bundles/bundle-pricing/

6 David Okwi (2015), Unlimited Internet Uganda: Vodafone's Unlimited Internet package could be the best we know, Dignited, February 10, 2015, http://www.dignited.com/12073/unlimited-internet-uganda-vodafones-unlimited-internet-package-best-know/

7 Poverty Status Report 2014; Structural Change and Poverty Reduction in Uganda, Ministry of Finance, Planning and Economic Development (2014), http://www.finance.go.ug/index.php?option=com_docman&Itemid=7&task=doc_download&gid=423

8 World Bank (2015) Uganda Country Profile, http://data.worldbank.org/country/uganda

Currently under a multiparty governance system, the country has 29 registered political parties and to date two general presidential elections have been held with the next due to take place in February 2016. However, allegations of voter intimidation and rigging have been cited by opposing parties.

Growing access and affordability of ICT and the attendant benefits it offers citizens could, be undermined by laws that subtract from citizens' privacy and the protection of their data. Notably, the Data Protection and Privacy Bill, 2014 falls short of protecting the privacy of Ugandan citizens. And, if passed in its current form, it would not be the only law in Uganda to breach citizens' rights which the country is obliged to uphold under both national laws and international instruments.

Uganda is a signatory to the Universal Declaration of Human Rights, which provides for freedom of expression and the right to privacy under Article 19 and 12, respectively.[9] Article 19 states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Article 12 states; "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.''

The country is also a signatory to the International Covenant on Civil and Political Rights, wherein Article 17 (1) affirms that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and (2) "Everyone has the right to the protection of the law against such interference or attacks."[10]

Similarly, the Constitution of the Republic of Uganda provides for the right to freedom of expression and speech, privacy and access to information under Article 29 (1) (a)[11], 27 (2) and 41[12] respectively. Article 27 (2) states, "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

In this brief, we review various ICT-related laws in Uganda and how they uphold or undermine the privacy of citizens. The laws reviewed include; the Regulation of Interception of Communication Act, the Computer Misuse Act, the Anti-Pornography Act, and the Uganda Communications Act, 2013. The review results are grouped under various privacy or internet rights issues and how they are affected by the country's laws.

9 Universal Declaration of Human Rights, http://www.un.org/en/documents/udhr/

10 International Covenant on Civil and Political Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

11 Article 29 (1) (a) "every person shall have the right to freedom of expression and speech which includes freedom of the press and other media."

12 "Every citizen has a right of access to information in the possession of the state or any other organ of the state except where the release of the information is likely to interfere with the security of the state or the right to the privacy of any other person."

Surveillance and Interception of Communications

Unless it is prescribed by law, necessary to achieve a legitimate aim and proportionate to the aim pursued, communication surveillance is a violation to privacy as a human right.[13] In Uganda, Sections 79 and 80 of the Communications Commission Act, 2013 criminalise infringing privacy and provides for the punishment of unlawful interception and disclosure of communication by a service provider. Communications services or systems providers and their employees are prohibited from (a) unlawfully intercepting any communication sent through their systems; (b) unlawfully interfering with or obstructing any radio communication; or (c) unlawfully disclosing any information in relation to a communication of which that operator or employee is aware. Offenders are liable to a fine not exceeding UGX 2.4 million (US$ 705) or imprisonment not exceeding five years or both.

Section 18 of the Computer Misuse Act, 2011 also upholds individuals' right to privacy of communications. It provides for the safety and security of electronic transactions and information systems, and criminalises unauthorised access to computer systems and data.

Despite these positive provisions in securing privacy rights and protecting data, the same laws also have negating provisions. Section 28 subsection 5 (c) of the Computer Misuse Act, 2011 gives powers to an "authorised officer"[14] who has a search warrant to "compel a service provider, within its existing technical capability - (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorities in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system."

The Regulation of Interception of Communications Act, 2010 provides for lawful interception of communications. According to this law, lawful interception can only take place after issuance of a warrant by a judge if there are "reasonable grounds" for interception to take place. This includes; "an actual threat to national security or to any national economic interest, a potential threat to public safety, national security or any national economic interest, or if there is a threat to the national interest involving the State's international relations or obligations."

The Regulation of Interception of Communications Act was enacted in pursuit of the Anti-Terrorism Act of 2002.[15] The anti-terrorism law gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance. Interception of communications may be conducted on grounds such as: safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism.

Further, the law under Section 3 mandates the ICT Minister to set up and administer a monitoring centre to facilitate collection of user' data. In 2013, then Security Minister announced government plans to set up 'social media monitoring centre.' The centre would allow monitoring users purportedly bent to cause harm to the government.[16] No further details have emerged about the existence of centre.

Although both the Regulations of interceptions of communications and the Anti–Terrorism Act provide for lawful interception of communications, it is not clear how collected user data is used and how its privacy is protected. This lack of transparency in the use and scope of communication surveillance violates the principle of transparency and user notification under the International Principles on the Application of Human Rights to Communications Surveillance, which calls for states to be transparent about the use and scope of communications surveillance laws, regulations, activities, powers, or authorities.[17] Besides, the absence of a proper definition of "national security" and it's increasing use to justify surveillance makes the concept vulnerable to manipulation by the States as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists.[18] Use of national security as grounds for surveillance may also often "warrant unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."[19]

13 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2013, A.HRC.23.40 EN, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

14 Computer Misuse Act Article 29 (9) an "authorised officer" is defined as a police officer who has obtained an authorising warrant.

15"The Anti-terrorism Act No.14 of 2002, "http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf

16 Francis Emorut, " Gov't plans to monitor social media," New Vision, May 31, 2013, http://www.newvision.co.ug/news/643403-gov-t-plans-to-monitor-social-media.html

17 International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/

18 See: Frank La Rue, 2013

19 Ibid. 19

Uganda is one of the African countries that have sought details on social media users. Between July and December 2013, the government sought for details from Facebook on one of its users.[20] In the first half of 2015, government made another request seeking details of two users.[21] The requests were denied by Facebook. It is not clear which government agency made the requests.

The Uganda Communications Act 2013 under Section 86 subsection 1 (a), gives power to the Uganda Communication Commission (UCC) to "direct" network operators to operate in a specified manner in order to alleviate the state of emergency." In April 2011, the regulator issued a directive to service providers to temporarily block access to use of certain services such as Facebook and Twitter in fear of networks being used to escalate violence. The order came in the heat of the 'walk to work' protests in various towns over rising fuel and food prices.[22] The UCC Executive Director stated that "the freedom to live is more important than, the freedom to express oneself" and that he would again order the two social networks to be cut off if it was in the interest of public safety.[23] Some service providers reported that they did not respond to this directive saying that it was received after the 24hour period during which they had been ordered to block access to the social networks.[24]

In July 2015, reports emerged that the Uganda Police Force and the Office of the Presidency were in advanced stages of acquiring hi-tech surveillance software from Israel and Italy to begin large-scale spying in Uganda.[25] Information disclosed by Wikileaks shows email exchanges between the Italian surveillance malware vendor, Hacking Team and its vendor, Zakiruddin Chowdhury, with strong contacts in Uganda.[26]

Anonymity

The internet enables anonymity of communications as it allows individuals to express themselves freely with little fear of retribution. Thus for users to exercise their right of privacy on the internet, they must be able to ensure that their communications remain private, secure and, if they choose, anonymous.[27] Anonymity also enables social participation and fosters freedom of expression online for journalists, activists and civil society groups who are subjected to both state and non-state actors attacks and interference.[28]

However, communications anonymity is compromised in Uganda with the mandatory registration of SIM cards as provided for under the Regulations of interception of communications, 2010. Users are required to provide personal information such as name, national ID, passport photo, place of birth, next of kin, resident and employment addresses.[29] This law provides service providers with access to huge databases of user information which poses a threat to anonymity and has the potential to enable location tracking, thus simplifying communication surveillance.[30] The lack of a data protection and privacy law, coupled with past documented online attacks such as targeted hacking, cyber bullying and harassment[31], underline the need for at-risk groups such as journalists and human rights defenders to be able to stay anonymous online.

20 Facebook, "Global Government Requests Report," Uganda Requests for Data, July – December 2013, https://govtrequests.facebook.com/country/Uganda/2013-H2/.

21 Facebook, "Global Government Requests Report," Uganda Requests for Data, January – June, 2015, https://govtrequests.facebook.com/country/Uganda/2015-H1/#

22 The New Vision, Profile: Walk-to-work campaign, April 02, 2012, http://www.newvision.co.ug/news/630112-profile-walk-to-work-campaign.html

23 Reporters without Boarders, April 20, 2011, Government could target Facebook and Twitter on eve of new protests, http://en.rsf.org/uganda-government-could-target-facebook-20-04-2011,40068.html

24 Open Net (2011), Government blocks Facebook, Twitter,",https://opennet.net/blog/2011/04/ugandan-government-asks-isps-block-facebook-twitter

25 Police in Shs 5bn spy deal, The Observer Uganda, http://observer.ug/news-headlines/38889-police-in-shs-5bn-spy-deal

26 Wikeleaks (2015), The Hacking Team - Re: R: I: Uganda Police, https://wikileaks.org/hackingteam/emails/emailid/11829

27 See: Frank Ra Lue (2013)

28 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2015, A/HRC/29/32, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

29 UCC, Sim Card Registration, http://www.ucc.co.ug/data/smenu/23/SIM-Card-Registration.html

30 See; Frank La Rue (2013)

31 Freedom House (2015), Uganda Freedom on the Net, https://freedomhouse.org/report/freedom-net/2015/uganda

Cybercrime

The need to fight increasing crimes committed online like e-fraud, hate speech, cyber stalking, hacking, child pornography, espionage, copyright infringement and online violence against women has made online data protection and privacy a necessary requisite for individuals, private companies and states. In Uganda, the e-Transactions Act (2011), E-Signatures Act (2011), Computer Misuse Act (2011) and the Anti-Pornography Act, 2014 were enacted to address these challenges.

The Computer Misuse Act, 2011 under Section 18 provides for the safety and security of electronic transactions and information systems, and criminalises unauthorised access to computer systems and data. For instance, according to Section 18 (1), "A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence." Offenders under this clause are punishable upon conviction with a fine not exceeding UGX 4 million (US$ 1,176), imprisonment not exceeding 10 years or both.

In 2012, three individuals were charged under the Computer Misuse Act. They were accused of unauthorized use and interception of computer services; electronic fraud; unauthorised access to data; and producing, selling or procuring, designing and being in possession of devices, computers, computer programmes designed to overcome security measures for protection of data.[32]

However, the Computer Misuse Act has also been used as an instrument to curtail voices critical of government online. In June 2015, police arrested and charged the person assumed to operate the pseudonym Tom Voltaire Okwalinga (TVO), who was accused of leaking government secrets on Facebook.[33] Robert Shaka was charged with using computers and other electronic devices to issue "offensive communication" against the first family and the Inspector General of Police[34] under Section 25 of the Computer Misuse Act, which states;

> *"Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor."*
>
> *A conviction attracts a fine not exceeding UGX 480,000 (US$140), imprisonment not exceeding one year, or both*

The Anti-Pornography Act, 2014 was enacted to curb pornography including online, however the law has been used to order the arrest of victims of revenge pornography. In November 2014, the Ethics Minister ordered the arrest of a local female music artist over her nude pictures which circulated widely on social media after supposedly being leaked by her estranged boyfriend.[35] Although she made a statement with the police, no charges were placed. The regulator has also threatened to shut down social media platforms used to promote pornographic content.[36]

Earlier in 2013, a National Computer Emergency Response Team was established to curb cybercrime and in 2014, rights activists critical of the unit reported that the police, through the unit, were profiling internet users deemed to be government critics.[37] Government did not respond to these allegations.

32 Republic of Uganda, Anti-Corruption Division, HCT-00-AC-SC-0084-2012, http://www.ulii.org/files/UGANDA%20V%20GUSTER%20NSUBUGA%20AND%203%20OTHERS.docx

33 Tom Okwalinga, https://www.facebook.com/tom.okwalinga

34 Anthony Weska & Ephraim Kasozi (2015), Museveni social media critic sent to Luzira, The Daily Monitor, June 12, 2015, http://www.monitor.co.ug/News/National/Museveni-social-media-critic-sent-to-Luzira/-/688334/2748626/-/35oekd/-/index.html

35 http://www.monitor.co.ug/News/National/Desire-Luzinda-should-be-locked-up-and-isolated--Lokodo/-/688334/2510248/-/iv07br/-/index.html

36 Moses Ndhaye (2015), UCC threatens to shut down social media platforms over abuse, The Daily Monitor, February 10 2015, http://www.monitor.co.ug/News/National/UCC-social-media-platforms-abuse/-/688334/2619032/-/151o4ktz/-/index.html

37 Unwanted Witness Uganda, "The Internet: They Are Coming For It Too," January 17, 2014, Page 38.

Intermediary Liability

Intermediaries such as ISPs, telecommunication companies and social media platforms are often used by governments to facilitate surveillance and censorship of online content. In many countries, existing legal requirements, practices and policies pertaining to intermediary liability are making it easier to enable surveillance of user undertakings online.[38]

In Uganda, certain laws like the Electronic Transactions Act, 2011 do not require service providers to monitor stored or transmitted data or to actively seek for facts or circumstances indicating unlawful activity. Section 29 of the Electronic Transactions Act exempts service providers from liability in respect to third party material in form of electronic records where he or she merely provides access, if liability is founded on (a) "the making, publication, dissemination or distribution of the material or a statement made in the material;" or (b) "the infringement of any rights subsisting in or in relation to the material".

Despite this positive provision, other laws like the Computer Misuse Act, 2011 and the interception of communications law have provisions that negate users' privacy. As mentioned earlier, Section 28 subsection 5 (c) of the Computer Misuse Act, 2011 gives powers to authorities to compel service providers to cooperate in the collect or recording of subscriber communications including in real time. Section 8 of The Regulation of Interception of Communications Act 2010 compels service providers to have their systems render real and full time capabilities by offering all call-related information for a party under surveillance. Failure to comply could lead to a possible conviction, a fine or imprisonment for a period not more than five year and possible cancellation of their licenses.

Meanwhile, the Anti-Pornography Act, 2014 – under Section 7 (f) provides for establishment of a Pornography Control Committee whose functions include to "expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography." The Act prohibits the production, traffic in, publishing, broadcasting, procuring, importing, exporting and selling or abetting any form of pornography. This law requires service providers to take measures recommended by the Pornography Control Committee, including installing software to detect and censor pornography. Under Section 17 (1) of this Act, ISPs whose systems are used to upload or download pornography can be imprisoned for five years and fined UGX 10 million (US$ 2,941). Subsequent conviction of the ISP may lead to the suspension of their operating license.

The Data Protection and Privacy Bill, 2014

As explained in the preceding sections, many of Uganda's laws negate the privacy of citizens' communications and data. While the proposed Data Protection and Privacy law seeks to protect the privacy of the individual and personal data by regulating the collection and processing of personal information, numerous clauses undermine privacy as outlined below.

Ambiguous Terminologies

The use of terminology that does not succinctly specify a role or action creates opportunity for the misuse of the law as seen in the definitions below:

Definition of proper performance, public duty and national security: Section 4(2) presents broad terminology that is open to misinterpretation by users. It states that personal data may be collected or processed where the collection or processing is necessary (i) for the proper performance of a public duty by a public body and for (ii) national security. The phrases, "proper performance" and "public duty" require specific qualification as they are open to abuse due to their broad definitions. Unspecified matters of "national security" could also permit the collection of data directly from a data subject in Section 7, thus leaving citizens' information open to unwarranted access.

Definition of religious or philosophical beliefs, political opinion, health or sexual life: Section 5 (1) of the Bill further allows for widespread collection and processing of personal data, placing restrictions only on data related to "religious or philosophical beliefs, political opinion, health or sexual life." This clause leaves room for collection and processing of personal data outside of these restrictions.

38 Elonnai Hickok (2014), Intermediary liability and state surveillance, https://www.giswatch.org/sites/default/files/intermediary_liability_and_state_surveillance.pdf

Definition of privacy infringement: 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." But no clear definition of what constitutes "privacy infringement" is provided. The lack of this defintion is likely to leave users' data open to abuse by data collectors and processors.

Definition of necessary, relevant and excess data: The type and amount of data that can be requested and stored by a data collector 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 that defines "excess data."

Definition of prescribed manner and prescribed fee: In its current form, the bill possesses unclear definition through which personal information is accessed. 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. It is not clear what constitutes the "prescribed manner" through which to make requests. Still under this section, requesters are required to pay a "prescribed fee" as a requirement to receive information. However, the amount to be paid is not stated. The Bill thus needs to state a minimal amount of money that can be paid to access personal data.

Data Accessibility, Retention and Security

According to Section 7 (2) (g) "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.

Besides, the length of time that collected personal data can be retained is not indicated and raises concern about the security and legitimate use of individual's personal 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. The retention of data for national security purposes again raises concern for the security and use of personal data as here too, national security is not defined.

Further, the Bill does not indicate the guarantee of the security of data due to be collected although Section 9 (1) 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. Although Section 15 provides for security measures to be undertaken by a data controller, it is not clear what happens when they do not provide security measures for data stored. Section 17 does not state what happens when a data controller discloses data unlawfully. The penalties for defaulters of these clauses are also not clearly stated.

Section 18 on 'notification of data security breaches' provides for immediate notification of a data subject should a breach occur. However, it further needs to specify a timeframe within which a data controller should notify a data subject after getting knowledge of the breach.

Further Section 19 (9) does not indicate a timeline within which a data subject should receive a response from the data controller. Besides, the maximum 30 days proposed for a data controller to comply with a request is too long and should be reduced to no more than 10 working days.

Meanwhile, the Bill provides for publishing of a breach on the website or in mass media. However, this 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 thus proposed in the Bill should not be employed if any 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.

Jurisdiction

The borderless nature of the internet and existence of service providers operating in more than one country makes it possible for communications and service providers to access data outside the jurisdiction of Uganda. The Bill in its current form does not address protection of data collected by data processors or controllers operating beyond Uganda's borders but utilising data belonging to Ugandan citizens or organisations. This needs to be clearly addressed in the Bill.

Data Formats, Notification and Release Period

The Bill provides for accessing information in the Data Protection Register under Section 26, but it does not specify the formats in which the public can access this information. Data access is also mentioned under Section 19, where requesters are required to pay a 'prescribed fee' to access data but the format under which this data can be accessed are not mentioned. The Bill thus needs to provide for such formats and suggested formats may include: electronic, print or verbal.

The 14 days provided for in Section 20 (2) for notification of compliance, notification of intent or non-compliance to prevent processing are too many, as within that period further processing could potentially be ongoing.

In addition the Authority should issue quarterly public reports on registered data collectors and the nature of any breaches recorded.

Unclear Remedies for Violators

The Bill does not provide for an appeal process to the data subject in the event of non-compliance with a request to prevent further processing of personal data if the Authority is not satisfied that the data subject's request is justified. The appeal process is also not specified for data subjects who want to prevent the processing of personal data for direct marketing.

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. The same Section does not specify compensation mechanisms for victims of privacy violations. It does not specify how compensation will be determined nor does it indicate the means of compensation.

The Bill under Part VIII does not specify a penalty for a data processor/ collector who through omission (such as negligence) or commission fails to secure a data subject's data, leading to its falling into unauthorised hands. This needs to be addressed.

Further, although the Bill provides for dispute handling through the Authority – in this case the National Information Technology Authority (NITA –U), an independent tribunal rather than the Authority as proposed in the Bill should settle cases that may arise in the event of no consensus between the data controller and data subject.

Conclusions

Uganda has made remarkable strides to promote ICT use among the citizenry. The adoption of the Cyber laws and their regulations appears to promise a safe haven for internet users. However, numerous provisions in the current legislation violate freedom of expression and opinion online, the right to access information and privacy.

As provided above, the drafting of the Data Protection and Privacy Bill, 2014 is a positive step towards addressing these privacy concerns but if passed in its current form, the Bill will not live up to the purpose it was created for.

Although an immediate passing of the Uganda Data Protection and Privacy Bill is recommended, the drafting phase should further engage with and seek consultations with different stakeholders including civil society, private sector, the media 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.

Existing laws such as the Electronic Signatures Act, 2011, the Computer Misuse Act, 2011, the Regulation of Interception of Communications Act 2010 and the Communications Commission Act 2013 which have a bearing on individuals' privacy and data protection should be amended to repeal contradictory provisions. Broad terminologies in these laws should be specifically clarified within the Data Protection and Privacy Bill in the contexts of user data, data collectors and data controllers to prevent abuse.

Whereas privacy and data protection challenges are largely associated with the state and service providers, the emerging threat of hackers and fraudsters should equally not be overlooked. Awareness raising and capacity building in digital safety and securing communications amongst users is paramount.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
156-158 Mutesa II Road, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org