State of Internet Freedom in Africa 2018

Privacy and Personal Data Protection: Challenges and Trends in Uganda

September 2018

CIPESA

Table of Contents

State of Internet Freedom in Africa 2018
Data Protection and Privacy: Challenges and Trends in Uganda

Creative Commons Attribution 4.0 Licence
‹creativecommons.org/licenses/by-nc-nd/4.0›
Some rights reserved.

1 Introduction and Background

Privacy is a fundamental human right that is enshrined in various international human rights instruments including the Universal Declaration of Human Rights (article 12); UN Convention on the Rights of the Child (article 16); International Covenant on Civil and Political Rights (article 17); United Nations Convention on Migrant Workers (article 14); African Charter on the Rights and Welfare of the Child (article 10); and the African Union Principles on Freedom of Expression (the right of access to information) (article 4). Other African frameworks that address privacy issues include the Declaration of Principles on Freedom of Expression in Africa (2002) (Part V),[1] and the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa 2016.[2]

Since 2012, the Uganda government has been collecting massive personal data through a national SIM card registration process which has also been in tandem with a national drive for registration of persons for purposes of issuance of national identification documents. The country has also been grappling with harmonising the various laws which contain problematic provisions on data protection and privacy, such as the Regulation of Interception of Communications Act that provides for interception and surveillance of personal communication, and the Computer Misuse Act that regulates online communication.

Some provisions in these laws are retrogressive in an increasingly digitised Uganda. Reports from the communications regulator, the Uganda Communications Commission (UCC), indicate that as at June 2018, the country had 21.6 million mobile subscriptions representing a 56% penetration rate while internet penetration stood at 47.4%.[3]

It is against this backdrop that this study was conducted to assess the state of privacy and data protection in Uganda over the last five years. The study tracks key trends in the country, analysing major risk factors, mapping notable developments on data protection and privacy legislation and violations, and identifying measures that can positively influence the right to privacy and data protection in Uganda. The study aims to inform key actors, including government, the media, academia, civil society on the current legal, institutional and practice landscape as well as opportunities for advancing the right to privacy and data protection.

1 *Available at http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html*
2 *Available at http://www.achpr.org/sessions/59th/resolutions/362/*
3 *UCC, Post, Broadcasting and Telecommunications Market & Industry Q2 Report, 2018, https://www.ucc.co.ug/wp-content/uploads/2017/09/Communication-Sector-Performance-for-the-Quarter-ending-June-2018.pdf*

2 Methodology

This study adopted a qualitative research approach consisting of key informant interviews and desktop literature reviews, policy and legal analysis. The literature review was conducted so as to generate an understanding of the current debates and issues on privacy and data protection in Uganda. Hence, policy and legal frameworks on privacy and personal data protection were analysed. This was to establish how the policy and legal frameworks shape citizens' enjoyment of the right to privacy. The laws and policies analysed included those that govern the telecommunications sector, the media, social media, access to information, interception of communications, security and intelligence agencies, and law enforcement in general.

Further, interviews with purposively selected key informants were conducted. The key informants included persons working with private companies, telecommunication firms, Internet Service Providers (ISPs) and government Ministries, Departments and Agencies (MDAs). The MDAs included the Ministry for ICT and National Guidance, police, Uganda Registration Services Bureau, Electoral Commission and the Uganda Communications Commission. Other respondents were drawn from the media fraternity, social media activists, human rights defenders, consumers' associations, academics, lawyers and select individuals from the general public.

3 Country context

This section provides an overview of the country's context in terms of the political economy, the status of Information and Communications Technology (ICT) in the country, and the political environment.

3.1 Political Economy

Uganda is a landlocked country located in East Africa. According to the Uganda Bureau of Statistics (UBOS) 2014 population census, Uganda has a population of 37.7 million with over two thirds of the population aged 35 years and below.[4]

The liberalisation and deregulation of the economy in the 1990s saw the government open up formerly nationalised industries in communications, transport, health, education, among others to the private sector. This phase of economic reform led to economic growth averaging 7% per annum until recently when it declined due to a fall in commodity prices, political instability in Uganda's strategic neighbouring states such as the Democratic Republic of Congo and South Sudan, and pressures from demographic shifts.

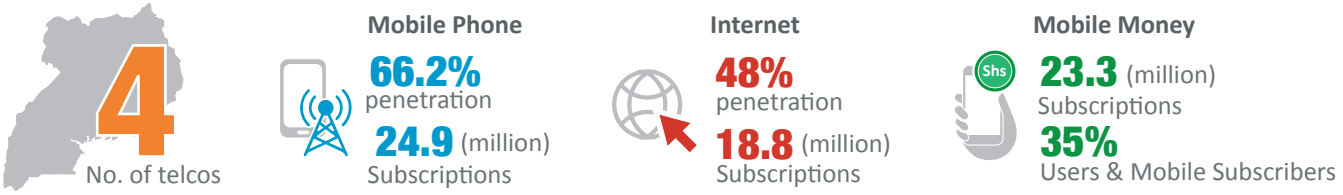
According to the World Bank, in 2018 Uganda had a gross domestic product (GDP) per capita income of USD 604[5] The services sector accounts for 51% of the GDP, while industry contributes up to 23%. Agriculture accounts for 25% of the GDP and it employs 69% of the working population.[6] More than 90% of the labour force employed in non-agricultural activities are in informal employment.[7]

3.2 ICT Status

The digital economy and generally access to the internet are important as they connect corporations, entities, individuals and governments. However, the internet's centrality comes with a number of challenges including interference with the right to privacy in today's networked society.[8]

4 *UBOS, National Population and Housing Census 2014, https://www.ubos.org/onlinefiles/uploads/ubos/NPHC/CENSUS%20FINAL.pdf*
5 *Available at https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UG*
6 *Available at https://data.worldbank.org/indicator/NV.AGR.TOTL.ZS?locations=UG ; https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS?locations=UG*
7 *UBOS (2013). National Labour Force Survey Report 2011/12, https://www.ubos.org/wp-content/uploads/publications/03_2018labour_report0203.pdf*
8 *Joshua Bryan Talamayan, "How Internet And Technology Changed The World," August 02, 2017, available at https://www.theodysseyonline.com/how-internet-and-technology-changed-the-world*

According to UCC, Uganda had 18.5 million internet users representing a penetration rate of 47.4%, as of June 2018. In the same period, there were 21.6 million mobile subscriptions representing a 56% penetration rate.[9] According to StatCounter, as of July 2018, Facebook was the most popular social networking site at 75.95%, followed by Pinterest at 13.39%, Twitter at 5.03%, YouTube at 3.7%, LinkedIn at 0.53%, and Google+ at 0.49%.[10] In Uganda, social media and mobile messaging are the entry point to internet use for many people.[11]



Summary of ICT figures in Uganda

3.3 Political Environment

Uganda has since 1986 been under the rule of President Yoweri Museveni's National Resistance Movement (NRM). There are concerns on the government's increasing surveillance capability over citizens' communications in the absence of data protection legislation. This is coupled with government hostility towards the political opposition and online critics especially through arrests and arbitrary prosecution.[12] Government has continually infringed on individual privacy and narrowed civic space through various activities including the alleged planting of FinFisher intrusion malware on hotel Wi-Fi to illegally spy on targeted persons;[13] enactment of restrictive legislation such as the Regulation of Interception of Communication Act and the Anti-Terrorism Act which among others permit interception of individuals' communications by government agencies.

In May 2018, the Uganda government passed a widely opposed amendment to the Excise Duty Act, introducing an excise duty tax of UGX 200 (USD 0.05) per user per day for use of Over-The-Top (OTT) services such as WhatsApp, Facebook and Twitter. The law became effective on July 1, 2018. The tax rendered the internet for Ugandans, particularly low income earners, less affordable.[14] Over and above that, Uganda's president Yoweri Kaguta Museveni has been outspoken about people using social media to spread what he terms as "lies and falsehoods".[15] Therefore, the tax has been widely seen as a move to limit freedom of expression online.[16]

9 *UCC, Post, Broadcasting and Telecommunications Market & Industry Q2 Report, 2018, https://www.ucc.co.ug/wp-content/uploads/2017/09/Communication-Sector-Performance-for-the-Quarter-ending-June-2018.pdf*

10 *Social Media Stats Uganda (July 2017 – July 2018), http://gs.statcounter.com/social-media-stats/all/uganda. It should be noted that Stats Counter does not directly account for "dark social" platforms such as WhatsApp and Telegram*

11 *CIPESA, State of internet freedom in Uganda 2015: Survey on access, privacy and security online, http://www.cipesa.org/?wpfb_dl=209*

12 *CIPESA, "Hunting Down Social Media 'Abusers' in Uganda as Elections Near," July 2015, available at https://cipesa.org/?wpfb_dl=190*

13 *Available at https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf*

14 *James Propa, "Social Media Blocked in Uganda Ahead of President Museveni's Inauguration," May 11, 2016, available at https://advox.globalvoices.org/2016/05/11/social-media-blocked-in-uganda-ahead-of-president-musevenis-inauguration/*

15 *Ibid.*

16 *Simone Schlindwein, "Uganda: One year of social media tax," July 20, 2019, available at https://www.dw.com/en/uganda-one-year-of-social-media-tax/a-49672632*

4 Laws and Policies Affecting Privacy and Personal Data Protection

This section gives an overview of the policy and legal framework for privacy and data protection in Uganda. It also highlights the international, regional and domestic legal framework and their implications on privacy and data protection in the country.

4.1 International Framework for the Protection of Privacy

As indicated in the introduction, Uganda is party to the key international human rights instruments which guarantee the right to privacy. These instruments include the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights whose articles 12 and 17 respectively provide for the right to privacy. Other relevant international instruments ratified and applicable to Uganda include the Convention on the Rights of the Child, the International Convention on the Protection of the Rights of all Migrant workers and members of their families.[17]

However, Uganda is still reluctant to express full commitment to the regional and international instruments. For instance, while African Union on June 27, 2014 adopted the African Union Convention on Cybersecurity and Personal Data Protection which is the main guiding instrument on privacy and personal data protection on the continent,[18] Uganda is yet to sign and ratify it.[19] Meanwhile, the East African Community (EAC) has not adopted a specific framework on data protection and privacy, but it was the first African regional economic community to develop a framework for cyber laws in 2008. The 2008 Framework for Cyber laws was meant to guide the EAC Member States on regional and national processes in order to facilitate a harmonised legal regime on electronic commerce and to curb unlawful conduct.[20]

4.2 The Constitution of the Republic of Uganda, 1995

The Uganda Constitution provides for the right to privacy under article 27. It protects persons from unlawful search of the person, home or other property of that person; unlawful entry by others on the premises of that person; and interference with the privacy of that person's home, correspondence, communication or other property. It should be noted that this protection extends to unlawful interception of correspondence or communication. The enforcement of this right requires enactment of an enabling law which is yet to be passed. Currently, the Data Protection and Privacy Bill, 2015 which is the proposed enabling law is yet to be passed.

17 *See also, Refugee Law Project, "International Conventions and Covenants," available at https://www.refugeelawproject.org/resources/relevant-resources/300-international-conventions-and-covenants*

18 *African Union, African Union Convention on Cyber Security and Personal Data Protection,https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.*

19 *African Union, List Of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection, https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf (accessed August 6, 2018).*

20 *Draft EAC legal framework for cyber laws https://bit.ly/2IhhR1i*

4.3 Recognition of Privacy and Personal Data Protection in Statutes

While Ugandans wait for the enactment of the Data Protection and Privacy Bill, 2015, privacy exists in various provisions which are scattered in various local legislation in Uganda. Some of these provisions are traceable in the: Computer Misuse Act, 2011;[21] Electronic Signatures Act, 2011;[22] Electronic Signatures Regulations, 2013;[23] Electronic Transactions Act, 2011; Electronic Transactions Regulations, 2013;[24] National Information Technology, Uganda (NITA-U) Act, 2009;[25] NITA-U (Authentication of IT Training) Regulations, 2016;[26] NITA- U (Certification of IT Providers and Services) Regulations 2016;[27] NITA-U (E-Government Regulations), 2015;[28] Anti-Terrorism Act, 2002 as amended 2015 and 2016;[29] Anti-Pornography Act, 2014;[30] Uganda Communications Act, 2013 as amended 2017;[31] and the Regulation of Interception of Communications Act, 2010.[32] It is important to note that some of the laws aforementioned recognise and protect the right to privacy while others limit the enjoyment of privacy.

4.3.1 Uganda Communications Act, 2013

The Uganda Communications Act regulates communication services in Uganda and provides for the establishment of the Ugandan Communications Commission (UCC),[33] whose functions include to monitor, inspect, licence, supervise, control and regulate communications services; receive, investigate and arbitrate complaints relating to communications services and take necessary action; establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators; and to set standards, monitor and enforce compliance relating to content.[34] The UCC under section 6 of the Act has a range of powers which include inter alia, charging of fees, imposing fines, classifying communication services and licences and confiscation of communication apparatus.

Further, the Act gives the Minister and the Commission, a wide range of powers, which have been severally used to interfere with the operations of the communications sector. For instance, in April 2018 the Commission issued a notice to all online data communication service providers requiring all online news platforms and online radio and television operators to apply and obtain authorisation for their online services.[35]

---

21 *Available at https://www.nita.go.ug/publication/computer-misuse-act-2011-act-no-2-2011*
22 *Available at https://www.nita.go.ug/publication/electronic-signatures-act-2011-act-no-7-2011*
23 *Available at https://www.nita.go.ug/publication/electronic-signatures-regulations-2013-si-43-2013*
24 *Available at https://www.nita.go.ug/publication/electronic-transactions-regulations-2013-si-42-2013*
25 *Available at https://www.nita.go.ug/publication/nita-u-act-act-no-4-2009*
26 *Available at https://www.nita.go.ug/publication/nita-u-authentication-it-training-regulations-2016-si-no-70-2016*
27 *Available at https://www.nita.go.ug/publication/nita-u-certification-it-providers-and-services-regulations-2016-si-no-69-2016*
28 *Available at https://www.nita.go.ug/publication/nita-u-certification-it-providers-and-services-regulations-2016-si-no-69-2016*
29 *The Anti-Terrorism Act, 2002 available at http://www.ulii.org/ug/legislation/act/2015/2002 ; the Anti-Terrorism Amendment Act, 2015 is available at http://chapterfouruganda.com/sites/default/files/downloads/The-Anti-Terrorism-Amendment-Bill-20151.pdf; the Anti-Terrorism Amendment Act, 2016 available at http://www.parliament.go.ug/new/images/Anti-Terrorism_amendment_Act_201621.pdf*
30 *Available at http://www.ulii.org/ug/legislation/act/2015/1-7, www.ug-cert.ug/files/downloads/The-Anti-pornography-act-2014*
31 *The Uganda Communications Act 2013 available at http://www.ict.go.ug/sites/default/files/Resource/UCC%20Act%202013.pdf ; the Uganda Communications Act 2013 (Amendment) Act, 2017 available at http://parliamentwatch.ug/wp-content/uploads/2016/10/The-Uganda-Communications-Amendment-Bill-2016.pdf*
32 *Available at http://www.ulrc.go.ug/system/files_force/ulrc_resources/regulation-interception-communications-act-2010.pdf?download=1*
33 *Section 4, UCC Act*
34 *Section 4, UCC Act*
35 *Available at http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf; See also, Daniel Mwesigwa, "Uganda Moves to Register Online Content Providers," March 25, 2018, available at https://cipesa.org/2018/03/uganda-moves-to-register-online-content-providers/ .*

Under section 79, the UCC Act criminalises the interception of communication between two people except within the confines of the law specified in section 86 and the Regulation of Interception of Communications Act, 2010. Under section 80, the same Act criminalises the interception of government communication or distraction of government from intercepting communication of. It should however be noted that the exceptions advanced for interception under the two provisions are a potential threat to individual privacy.

4.3.2 National Information Technology Authority Act, 2009

The National Information Technology Authority Act establishes the National Information Technology Authority Uganda (NITA-U) under section 3. Under section 5 of the Act, NITA-U's functions include creating and managing the national databank, monitoring and regulating data standards, and promoting and providing technical guidance for the establishment of e-Government, e-Commerce and other e-Transactions in Uganda.

Part V of the NITA-U Act regulates information technology surveys and powers of the authority. Section 19 stipulates that the minister may, on the recommendation of the board, issue a statutory order directing that an information technology survey be taken by the authority on both public and private sectors. In carrying out such a survey the authority has the power to collect information and data regarding information technology for the sector specified in the order. It may use summons and search warrants to facilitate the enforcement of such collections of data and information. Section 20 (1) stipulates that where data or information on information technology is being collected in accordance with Section 19, the Executive Director, an officer of the Authority, or an authorised officer, may require any person to supply him or her with any particulars as may be prescribed, or any particulars as the Executive Director may consider necessary or desirable in relation to the collection of the information.

Furthermore, a person who is required to give information under subsection 1, shall, to the best of his or her knowledge and belief provide all the necessary information, in the manner and within the time specified by the Executive Director. The powers of the authority are further expounded in Section 21, where it is stipulated that the staff of the Authority or an authorised officer may at all reasonable times enter and inspect any building or place and make such inquiries as may be necessary for the collection of information and data for a survey being carried out under Section 19.

4.3.3 Registration of Persons Act, 2015

The Registration of Persons Act was passed to harmonise and consolidate the law on registration of persons. Section 4 of the Act establishes the National Identification and Registration Authority (NIRA) which is mandated under section 5 to register citizens and non-citizens and births, issue unique identification numbers to persons registered, and also issue national identity cards.

As part of its mandate, NIRA in April 2014, together with the UCC embarked on a nationwide issuance of identity cards which entailed, among others, the collection and processing of personal data before issuance of cards.[36] The NIRA's mandate includes ensuring the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register. National IDs contain a series of demographic and biometric data such as names, sex, profession, religious belief, address, age and tribe of the data subject. The Act provides that the information in the register shall be used for, among others, national security, law enforcement, public administration, and providing social services. However, there are no clear regulations under the Act on how NIRA is expected to ensure the protection and security of the information collected.

By April 4, 2017, 14.8 million citizens have been registered and issued with IDs.[37] In the same month on the 12th, the UCC issued a seven day ultimatum for subscribers to update their SIM card registration details using National Identity Cards (IDs) in a move widely seen by authorities as a panacea towards the recent wave of crime executed with the help of mobile phones and the increasing trends in cybercrime.[38]

4.3.4 The Computer Misuse Act, 2011

The Computer Misuse Act aims to protect the safety of electronic transactions and information systems. Under sections 3 and 6, the Act makes strides in regulating access to data held on computers providing for protection and prohibition of unauthorised access. Further, it provides for cases where access and modification may be deemed unauthorised, under sections 8 and 12 respectively. Under the Act, computer misuse offences include unauthorised access (section 13); unauthorised modification of data (section 14); unauthorised use or interception of computer services (section 15); unauthorised disclosure of access codes (section 17); and unauthorised disclosure of information (section 18).

The Act also emphasises the need for authorisation before the interception of computer services (section 15); obstruction of use of computer (section 16); disclosure of codes (section 17); and information disclosure (section 18). These sections reveal that while privacy is provided for, it may be taken away under authorisation. The Act also outlaws electronic fraud under section 19. It also provides for punishment for computer-related offences under section 20. The Act further legislates against cyber harassment (section 24); offensive communication (section 25); and cyber stalking (section 26).

The Act makes provision for preservation orders for data in cases of data vulnerability or loss, under section 9. Further, under sections 9 and 11, investigation officers may apply for orders of investigation and production of data for purposes of criminal investigations. The Act also provides for search and seizure on orders of a Magistrate.

---

36 *Richard Wanambwa, "Registration for National IDs Starts," Daily Monitor April 13, 2014, available at https://www.monitor.co.ug/News/National/Registration-for-national-IDs-starts/688334-2278502-od3osqz/index.html*

37 *Brigadier Stephen Kwiringira, "Integration of Services with the National Identification System, Uganda's case," Presentation at the 3rd Annual Conference for the ID4Africa Movement, Windhoek, Namibia April 2017 available at http://www.id4africa.com/2017_event/Presentations/1-2-5_National_Identification_and_Registration_Authority_Brig._Stephen_Kwiringira.pdf*

38 *Edrine Wanyama, "The Stampede for SIM Card Registration: A Major Question for Africa," April 18, 2018, available at https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/*

Notably, this Act has previously been used to suppress voices critical of the government evidenced in the arrest and prosecution of social media critic Dr. Stella Nyanzi who is accused of cyber harassment and offensive communication under sections 24 and 25 of the Act.[39] On January 27, 2017, Dr. Nyanzi took to her Facebook account and allegedly said that the President of Uganda was 'a pair of buttocks' in reaction to the President's comments that he was 'not anybody's [public] servant but just a freedom fighter' the previous day while presiding his party's 31st anniversary in power.

4.3.5 Regulation of Interception of Communications Act, 2010

The Regulation of Interception of Communications is largely the instrument that facilitates infringement with individual privacy by permitting interception of communications. It provides for the lawful interception and monitoring of communications in the course of their transmission through telecommunication media or postal services or any other service.[40] Section 2 of the Act bars unlawful interception of communication by any person save for where there is consent or an authorised warrant. Despite the protection guaranteed in section 2, section 3 establishes a monitoring centre for the interception of communications.

Further, the Act lists a number of individuals who are authorised to apply for a warrant of interception to a judge as including the Chief of Defence Forces or their nominee; Director General of the External Security Organisation or their nominee; Director General of the Internal Security Organisation or their nominee; and the Inspector General of Police or their nominee. Further, section 5 alongside sections 6, 7, 8, 9, 10, 11 and 12, indicate that interception of communications may be authorised by a judge in as far as such information may be considered as life threatening, relates to drugs and human trafficking, poses actual actual threat to national security, public safety or to any national economic interest State's international relations or obligations. Further, section 11 also requires providers of postal or telecommunications systems to provide telecommunication service which have the capability of being intercepted.

4.3.6 The Electronics Signatures Act 2011

The Electronics Signatures Act regulates the use of electronic signatures. Section 81 provides for the obligation of confidentiality. It is to the effect that no person shall obtain access to any electronic record, book, register, correspondence, information, document, other material or grant access to any other person unless under the order of court. Further, the Act, under section 86, provides for a search warrant which may be granted by a magistrate to a police officer not below the rank of Inspector to enter premises and carry out a search. On the other hand, such police officers may forego the warrant and search the premises under section 87 of the Act where there is a delay in obtaining a search warrant and a likelihood of tampering with, removal, damage or destruction of subject evidence. These provisions of the Electronic Signatures Act affect freedom of expression online as well as the right to privacy online.

---

39 *Joseph Kato & Derrick Wandera, "Dr Nyanzi arrested over offensive communication," April 08, 2017, available at http://www.monitor.co.ug/News/National/Dr-Nyanzi-Janet-Museveni-Education-pad-schools-offensive/688334-3882326-oik0hh/index.html.*

40 *Regulation of Interception of Communications Act, 2010. Long title.*

4.3.7 The National Information and Communications Technology Policy for Uganda Policy, 2014

In 2014, the government of Uganda adopted the National ICT Policy with the aim of enhancing the telecommunications, postal services, broadcasting, information technology and information management services for economic development and transformation of the country. The policy identifies and lists some of the government strategies, such as developing legislation to address privacy and data protection of the individual in all spheres of life.[41] The areas covered by the policy include health, e-commerce and consumer protection, information security and education. However, this policy is yet to be fully implemented, especially in the absence of a specific operational law on privacy of the individual to guarantee data protection.

4.3.8 Guidelines and ICT Standards

Besides the use of laws and policies, there are other guidelines and ICT standards which are highly recommended for ensuring privacy. For instance, the government through NITA-U issued guidelines that require government ministries, departments and agencies (MDAs) to issue disclaimers alerting users when they are no longer on a government site and that the site's own privacy policy applies. Further, the guidelines require MDAs to guard against identity theft, respect the privacy of others, choose more secure modes of communication and to report all cases of abuse or misuse of social media platforms.[42]

Further, NITA-U has put in place a number of guidelines such as the NITA-U Standards Catalogue, 2017;[43] the Online E-Safety Educational Toolkit for Young People in Uganda;[44] Guidelines for Development and Management of Government Websites;[45] Guidelines for Operation, Usage and Management of IT Infrastructure in MDAs & Local Government;[46] Standards for Structured Cabling for Government MDAs;[47] and the Guidelines and Standards for Acquisition of IT Hardware & Software for MDAs.[48]

41 *The National Information and Communications Technology Policy for Uganda Policy, 2014, http://www.ict.go.ug/sites/default/files/Resource/ICT_Policy_2014.pdf*
42 *"Government of Uganda Social Media Guide," Pp.18, available at https://www.nita.go.ug/sites/default/files/publications/Government-of-Uganda-Social-Media-Guide.pdf (accessed August 7, 2018).*
43 *Available at https://www.nita.go.ug/publication/nita-u-standards-catalogue-2017*
44 *Available at https://www.nita.go.ug/publication/online-e-safety-educational-toolkit-young-people-uganda*
45 *Available at https://www.nita.go.ug/publication/guidelines-development-and-management-government-websites*
46 *Available at https://www.nita.go.ug/publication/guidelines-operation-usage-and-management-it-infrastructure-mdas-local-government*
47 *Available at https://www.nita.go.ug/publication/standards-structured-cabling-government-mdas*
48 *Available at https://www.nita.go.ug/publication/guidelines-and-standards-acquisition-it-hardware-software-mdas*

5 Results: Status, Trends and Challenges

This chapter details the emerging trends and key challenges to privacy and personal data protection in Uganda, citing various examples and incidents from the country.

5.1 Limited Understanding of Privacy

Despite provisions in the constitution and other laws on privacy of the individual, a large majority of Ugandans remain unaware of their rights both in the physical and cyber realms.[49] The understanding of privacy is varied within different social, political and cultural contexts. Limited understanding of privacy was further shown in individual perceptions of what one considers private. For example, according to a lawyer interviewed for this report, taking and sharing photographs of a bride and groom at a wedding ceremony might be celebratory and not a matter of privacy. This raises a number of concerns owing to the fact that such private information is usually shared on public platforms such as social media without the consent of the subject. Ideally, such actions lead to breach of individual privacy and therefore a human rights violation.

5.2 Fragmented Oversight Over Privacy Protection

A number of MDAs such as the Ministry of ICT and National Guidance, the National Identification and Registration Authority, the Ministry of Internal Affairs, the Uganda Registration Services Bureau, the Electoral Commission, the Uganda Communications Commission, the Ministry of Finance, Planning and Economic Development, the Uganda Investment Authority, National Enterprise Corporation, the Financial Intelligence Authority, the Uganda Revenue Authority, the Uganda Bureau of Statistics and the Bank of Uganda are charged with functions that involve mass collection of personal data from individuals in the absence of proper data protection and privacy mechanisms and policies. Moreover, there is no specific law on the protection of individual data and privacy. Notably, the Ministry of Gender, Labour and Social Development collects data relating to children and youth affairs, employers and employees, the elderly and persons with disabilities but has no clear accountability mechanism.

The legislative policy frameworks framework reveal weak enforcement of the laws as well as weak compliance. In June 2018, MTN Uganda's data centre in Mutundwe, Kampala was unlawfully raided by security personnel belonging to the Internal Security Organisation (ISO), a national security intelligence agency, in a counter-intelligence operation on MTN's alleged role in spying on behalf of a foreign government.[50] The security personnel not only detained Moses Keefah Musasizi, a data facilities manager at Huawei Uganda contracted to manage physical access to the MTN Data Centre for four hours but also disconnected four servers hosting customer data on mobile money and micro-lending.[51] MTN said that the incident posed a serious security risk to their telecommunications infrastructure, customer data and privacy.[52]

49 *Hilary Hueler, "Barefoot' Lawyers Teach Ugandans Their Rights," May 30, 2014, available at https://www.voanews.com/a/barefoot-lawyers-teach-ugandans-their-rights/1926220.html*

50 *MTN Uganda data centre raided over security https://bit.ly/2ueGsgo*

51 *Monitor Reporter, "Trespassers break into MTN data centre, disconnect four servers," July 6, 2018, https://bit.ly/2NHRxTG*

52 *Security personnel raid MTN Uganda data centre, disconnect servers, https://www.the-star.co.ke/news/2018/07/06/security-personnel-raid-mtn-uganda-data-centre-disconnect-servers_c1783205; See also ISO Agents Failed to Penetrate Our Servers – MTN, https://chimpreports.com/iso-agents-failed-to-penetrate-our-servers-mtn/*

5.3 Privacy Breaches by Governments

5.3.1 The Twists and Turns of SIM Card Registration

The UCC embarked upon a mass SIM card registration process in 2012, citing the Regulation of Interception of Communications Act, 2010 which provides for registration of existing SIM cards.[53] The UCC justified the process citing it as as necessary to "[h]elp law enforcement agencies to identify the mobile phone SIM card owners", "[t]rack criminals who use phones for illegal activities", "[c]urb other negative incidents such as; loss of phone through theft, nuisance/hate text messages, fraud, threats and inciting violence", and "[h]elp service providers (network operators) know their customers better."[54] Without sufficient constitutional guarantees on data protection and privacy, the registration raised concerns within the public and media on mass surveillance and a threat to individual privacy.[55] Initially, in December 2013, the High Court declined to hear the case by Human Rights Network for Journalists-Uganda (HRNJ-Uganda) and Legal Brains Trust challenging the SIM card registration exercise. The Court argued that the SIM card exercise had ended on August 31, 2013 and that it would be futile to litigate retrospectively.[56] Further, in a High court ruling on May 18, 2017, judge Steven Musota dismissed another case filed by Norman Tumumbise and Trumpet Ug Ltd, seeking to block the UCC from deactivating all unregistered SIM cards by May 19, 2017.[57]

On April 12, 2017, the UCC issued a seven day ultimatum for citizen subscribers to update their SIM card registration details using only valid national Identity (ID) cards to curb the recent wave of physical and cyber crime allegedly executed with the help of unregistered mobile phones.[58] The Uganda Law Society termed this ultimatum as illegal citing, among other things, that the Registration of Persons' Act allows valid identification documents issued by government agencies such as national ID cards, work permits, passports, driving licence, student Identity cards and voter's cards to be used for registration.[59]

On March 28, 2018, UCC issued a directive banning the sale of new SIM cards with new guidelines requiring telcos to use national ID card readers to electronically verify registration data against the national ID register maintained by NIRA.[60] In April 2018, the Parliament resolved to extend the SIM card registration by not more than one year, however, Frank Tumwebaze, the Minister of ICT and National Guidance responded on Twitter that, "Government notes and will address issues of Parliament in regard to the SIM-card verification period, the deadline stands."[61] UCC, however, lifted the ban after NIRA gave them 50 biometric machines to facilitate the capturing of user biodata.[62]

53 *Available at http://web.archive.org/web/20131201000000*/https://www.ucc.co.ug/data/smenu/23/SIM-Card-Registration.html*
54 *Ibid.*
55 *Edrine Wanyama, "The Stampede for SIM Card Registration: A Major Question for Africa," April 18, 2018, available at https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/*
56 *HRNJ-Uganda, "Ugandan court declines to hear SIM card registration case," December 13, 2013, available at https://ifex.org/ugandan-court-declines-to-hear-sim-card-registration-case/*
57 *Vision Reporter, "Sim-card registration case dismissed," May 18, 2019, available at https://www.newvision.co.ug/new_vision/news/1453570/sim-card-registration-dismissed*
58 *Edrine Wanyama, The Stampede for SIM Card Registration: A Major Question for Africa, https://cipesa.org/2018/04/the-stampede-for-sim-card-registration-a-major-question-for-africa/*
59 *Stephen Kafeero, "New UCC Sim card registration directive illegal - Law society," April 15, 2017, available at https://www.monitor.co.ug/News/National/New-UCC-Sim-card-registration-directive-illegal-Law-society/688334-3890052-9ii9ai/index.html*
60 *Sydney Mugerwa, "UCC bans sale of SIM cards with immediate effect," March 28, 2018, available at https://www.dignited.com/29103/ucc-directive-telecoms-uganda-stop-sale-of-sim-cards/*
61 *The Independent, "Parliament resolves to extend SIM-card deadline to next year," May 18, 2017, available at https://www.independent.co.ug/uganda-parliament-extends-sim-card-deadline-next-year/*
62 *Available at https://twitter.com/IBbossa/status/984857246566895617*

Despite efforts to register SIM cards, crimes committed through use of mobile phones and the internet have not drastically reduced as expected. In fact, there have been recent cases of identity theft and cyber fraud committed through use of registered SIM cards. In 2018, SIM cards belonging to Members of Parliament (MP) were cloned and used in a SIM card duplication fraud, a sophisticated form of fraud that allows hackers to gain access and control a user's phone number. The Parliamentarians included Western Youth MP Mwine Mpaka and Eastern Youth MP Ishma Mafabi who reported how they were hacked in a similar manner where their numbers were used by hackers to solicit for funds from friends, colleagues, and family.[63]

5.3.2 Scaling up of Digitisation Programmes

subscribers to update their SIM card registration details using Managed by NITA-U, Uganda's e-government platform, also known as eCitizen, offers access to personal information in databases relating to 74 transactional services, ranging from eTax, Business registration, trading license registration and social security statements, among others.[64] As of August 2018, Uganda's eCitizen portal did not contain a privacy statement or policy on the website.

These efforts to transform public services through digitisation and the offer of e-services have resulted in consolidation of existing government databases and the collection of new data from citizens, including biometric data. The programmes are largely being implemented by third parties or through multilateral partnerships, for instance, the NIRA's national ID registration is implemented by a German firm, Mühlbauer, responsible for key technical and operational aspects of the exercise.[65] Hence, personal data of citizens are being handled by third party contractors outside government control. Moreover, there has been no assessment of the risk to privacy and personal data currently being handled by such contractors. Such programmes are continuously being scaled up despite the absence of a specific law on data protection and privacy.

5.3.3 State Acquisition and Deployment of Surveillance Technologies

In July 2018, the UCC installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks as well as mobile money transactions, fraud detection and billing verification.[66] The system is hosted on communications infrastructure owned by mobile network operators, and the UCC will be able to monitor multi-vendor data, network performance, and customer experience records, among others.[67] The president had long accused telecom companies of tax evasion and under-reporting revenues to the government.[68] In January 2018, it was revealed that the UCC had set up a Centralised Equipment Identity Register system in a bid to identify, and stamp out counterfeit and illegal mobile devices said to be hazardous to health and used to commit crime.[69] It should be noted that the government through the INMS has full access to critical telecom data such as call detail data and billing verification. This is because it facilitates interception of all transactions. Consequently, there are breaches in as far as clients or consumers transactions are concerned.[70]

63 *URN, "MPs losing millions to sim-card hackers," February 16, 2018, available at https://observer.ug/news/headlines/56945-mps-losing-millions-to-sim-card-hackers.html*
64 *Available at www.ecitizens.go.ug*
65 *Available at https://www.muehlbauer.de/company/contact/locations/uganda/*
66 *Franklin Draku, "Government Installs System to Track Telecoms Revenues," Daily Monitor July 3, 2018, available at https://www.monitor.co.ug/News/National/Government-installs-system-track-telecoms-revenues/688334-4643438-kql9ocz/index.html*
67 *Government installs system to track telecoms revenues, https://bt.ly/2OQDXU*
68 *All Africa, Uganda: Fight Over Shs44 Trillion Mobile Money, https://allafrica.com/stories/201802260042.html*
69 *Unwanted Witness, Uganda Communication Commission sets up mobile phone monitoring system, https://unwantedwitness.or.ug/uganda-communication-commission-sets-up-mobile-phone-monitoring-system*
70 *Franklin Draku, supra note 63.*

5.3.4 Increased Information Requests from Governments

In 2013, Uganda was among five African countries that made information requests to Facebook ranging from users' personal information to restrictions of certain content.[71] However, these requests were denied. Meanwhile, there was no substantial evidence that Uganda makes information requests to the telecom companies given the telecom companies such as MTN Uganda and Airtel Uganda do not produce transparency reports.

5.3.5 Revenge Porn and Breach of Individual Privacy

Ugandan socialite, Judith Heard, was arrested on July 31, 2018, over nudes and indecent video that were leaked on social media in May by her former boyfriend.[72] The police charged her for breach of the Anti-Pornography Act, 2014, which prohibits the production and consumption of pornography. Section 13(1) states: "A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any pornography." The fast growing cases of revenge porn thanks to jilted lovers and extortionists such as hackers, disportionately affect women more.[73] It should however be noted that the Act lumps the liability to the subject instead of the perpetrator. Meanwhile, the Anti-Pornography Act also requires ISPs to monitor online content to identify and remove content considered pornographic.

5.3.6 Office Break-Ins

Civil society organisations have faced several data protection threats and challenges in Uganda. Over time, there have been several reports of raids on premises of Civil Society Organisations (CSOs) by unknown parties who reportedly took mostly computer disks, serveras, computers and other electronic devices. Since 2012, there have been over 24 unsuccessfully investigated break-ins into premises of CSOs. These raids have led to loss of information and data held by CSOs.[74] Today, CSOs feel their data and information is at stake of being taken away in the shrinking data protection space.

71 *Tendai Mupaso, "Government requests report: 5 African governments request info from Facebook," April 17, 2014, available at https://www.techzim.co.zw/2014/04/government-requests-report-5-african-governments-request-info-facebook/*

72 *Joseph Kato, "Socialite Judith Heard arrested over leaked nude pictures," July 31, 2018, availabl eat https://www.monitor.co.ug/artsculture/Entertainment/Socialite-Judith-Heard-arrested-leaked-nude-pictures/812796-4690524-11wjah3z/index.html*

73 *Esther Nakazzi, "Revenge porn is rising and it should be addressed," March 13, 2015, available at https://www.opennetafrica.org/revenge-porn-is-rising-and-it-should-be-addressed/*

74 *Emmanuel Ainebyoona, Police on the spot as break-ins into NGO offices remain uninvestigated,, http://www.monitor.co.ug/SpecialReports/Police-spot-break-ins-NGO-offices-remain-uninvestigated-ACCU/688342-3843648-11dydsi/index.html*

5.4 Privacy Breaches by Business Entities

5.4.1 Legal Responsibility of Business Entities

According to the UN "Protect, Respect, and Remedy" Framework and Guiding Principles, business entities have a corporate responsibility to respect human rights by acting with due diligence to avoid infringing on the rights of others, and addressing harms that occur.[75] Further, section 79 of the UCC Act, 2013 bars telecom operators and ISPs or their employees from intercepting or unlawfully disclosing users' communications.

5.4.2 Targeted and Indiscriminate Communication

Internet and telemarketing are arguably a strategy employed by businesses and telecommunications companies in Uganda. There have been constant complaints by the general public to the UCC for annoying unsolicited messages and promotional calls they receive from telecom companies and marketers, even though UCC has regulations on SMS texts and messaging.[76] For instance, the Parliament and the Office of the Auditor General have cited incompetence on the part of UCC.[77] In some cases, unsuspecting subscribers have had to pay for a service they did not individually request for such as the receipt of messages from unknown or known channels but never voluntarily subscribed to. This has led to increasing public outrage since it interferes with individual peace and privacy and comes with economic costs.[78]

In 2015, the UCC in response to MTN's noncompliance imposed a fine of UGX 5 billion (USD 1.7 million) against MTN Uganda for breach of communication directives and non-compliance on cases including abuse of subscriber user data and defiance of a UCC directive to desist from using SMS short codes 157, 169, 178, and 183, billing platforms, anti-competitive behaviours and unacceptable subscriber data confidentiality practices.[79] The fine represented 0.5% of MTN Uganda's gross annual revenue and it is reported the company is seeking legal remedy.[80]

5.4.3 Mishandling of Customer Data

Confidential customer data has been leaked from various business entities by a range of actors. For example, the financial details of Justine Bagyenda, a former Director of Supervision at the Bank of Uganda (BoU), were allegedly leaked, according to a local news report, by bank and telco insiders.[81] MTN Uganda admitted that elements within their staff had undermined customer confidentiality and leaked Bagyenda's mobile money transaction details worth about UGX 500 million (USD 139,000) in the last three years.[82] In a public apology to Bagyenda, MTN also assured customers and the public that "all confidential customer information is handled and protected with the highest duty of care and integrity." MTN further noted that the staff in question had been handed over to relevant authorities to face criminal prosecution for their individual actions.[83] In March 2018, it

75 *Available at https://www.business-humanrights.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf*
76 *Available at https://www.ucc.co.ug/files/downloads/UCC%20GUIDELINES%20ON%20SMS%20and%20MMS.pdf*
77 *Lubowa Abubaker, "UCC on the spot over spam call and messages," Daily Monitor, October 24, 2018, available at http://www.monitor.co.ug/News/National/UCC-on-the-spot-over-spam-calls-and-messages/688334-2497288-6y91mp/index.html*
78 *Lubowa Abubaker, Ibid.*
79 *Daily Monitor, "MTN Uganda fined Shs5b for breach of UCC directives," Day Monitor March 3, 2015, available at https://www.monitor.co.ug/News/National/MTN-Uganda-fined-breach-UCC-directives/688334-2641212-wfdfbp/index.html; see also, David Rupiny, "MTN Uganda Weighing Legal Action over UCC UGX 5 Billion Fine," URN, March 5, 2015, available at https://ugandaradionetwork.com/story/mtn-uganda-weighing-legal-action-over-ucc-ugx-5-billion-fine*
80 *MTN Uganda Weighing Legal Action over UCC UGX 5 Billion Fine, https://bt.ly/2NISCLi*
81 *Business Focus Reporter, "Ex-BoU Boss Bagyenda's MTN Mobile Money Account Details Leak," March 27, 2018, available at http://businessfocus.co.ug/ex-bou-boss-bagyendas-mtn-mobile-money-account-details-leak/*
82 *George Okello, "MTN vows action against staff over Bagyenda Mobile Money transactions," April 6, 2018, available at http://www.pmldaily.com/news/2018/04/mtn-vows-action-against-staff-over-bagyenda-mobile-money-transactions.html*
83 *George Okello, "MTN vows action against staff over Bagyenda Mobile Money transactions," April 6, 2018, available at http://www.pmldaily.com/news/2018/04/mtn-vows-action-against-staff-over-bagyenda-mobile-money-transactions.html*

was reported that Bagyenda held UGX 19 billion (USD 5.27 million) in USD and UGX bank accounts in Diamond Trust Bank (DTB), Barclays Bank, and Centenary Bank. In separate press releases, DTB and Barclays Bank confirmed that actors within their staff had corruptly leaked Bagyenda's transaction details and tendered their apologies.[84] "[Barclays] has initiated necessary disciplinary proceedings against the employee responsible for unauthorised access to Bagyenda's accounts in line with the law and the bank policies."[85] The former BoU Director is already facing investigations by the Inspectorate of Government (IGG) over money-laundering and abuse of office.[86]

5.5 Dispute Resolution and Remedies

5.5.1 Notable Judicial and Quasi-Judicial Decisions

In cases of breach of privacy of the individual, a court may award damages to the aggrieved data subject or may order that the use of the continued breach stops forth with. The Courts have been progressive in this respect. In the case of Asege Winnie V Opportunity Bank & Anor,[87] Asege Winnie was awarded damages of over UGX 150 million (USD 41,600) in 2016, for among others, breach of her constitutional right to privacy and breach of confidence through the unauthorised use of her image in an advertising campaign dubbed "Agro Save". The facts of the case are that in 2013, she saw her image pasted on huge billboards run by Opportunity Bank in which Asege was shown to be heartily laughing and holding a bountiful harvest of oranges in her hands accompanied by the caption "Save for your success with the Agro Save Account". Besides the billboards, her image was reproduced for other advertising media such as brochures, flyers and calendars which were distributed across the country. The High Court found that the use of the defendant's image constituted intrusion of her privacy.

Meanwhile, the Uganda Communications Commission together with Uganda Media Council established by section 8 of the Press and Journalist Act Chapter 105 recently passed a decision which showed that the right to privacy of the plaintiff had been violated. In this decision, Faridah Nakazibwe brought a case against the Hello Tabloid and its editor Richard Tusiime on allegations of publishing 38 articles about her in the tabloid, causing her mental anguish and lowering her esteem in the eyes of her children, family and society. The Committee found that there had been a breach of the plaintiff's privacy and degradation of her dignity and awarded her Uganda shillings 45 million (USD 12,014.58).[88]

84 *Franklin Draku, "Leaked bank details: DTB apologises to Bagyenda," March 10, 2018, available at http://www.monitor.co.ug/News/National/Leaked-bank-details--DTB-apologises--Bagyenda/688334-4335696-12wep3e/index.tml*

85 *Ibid, see also, Ronald Mayanja, "Banks apologise to former BoU director over leaked account details," March 19, 2018, available at https://www.pmldaily.com/news/2018/03/banks-apologise-to-former-bou-director-over-leaked-account-details.html*

86 *George Mangula, "FIA on spot over failure to apprehend Bagyenda," May 28, 2018, available at https://eagle.co.ug/2018/05/28/fia-on-spot-over-failure-to-apprehend-bagyenda.html*

87 *Asege Winnie V Opportunity Bank (U) Ltd & Anor (HIGH COURT CIVIL SUIT NO. 756 OF 2013) [2016] UGCOMMC 39 (2 May 2016); available at https://ulii.org/ug/judgment/commercial-court/2016/39*

88 *Cecilia Okoth, Red Pepper to pay Faridah Nakazibwe sh45m,"https://www.newvision.co.ug/new_vision/news/1477666/red-pepper-pay-faridah-nakazibwe-sh45m ; see also URN, Red Pepper ordered to pay Shs 45m to NTV's Faridah Nakazibwe, https://observer.ug/news/headlines/57699-red-pepper-ordered-to-pay-shs-45m-to-ntv-s-nakazibwe.html.*

5.5.2 Progressive Steps

In March 2018 the Uganda Revenue Authority wrote to commercial banks requesting for access to all clients' bank records such as account name, Tax Identification Numbers (TINs) by which taxpayers are identified, National Identification Card Numbers (NINs), and contact details for the purposes of taxation purposes.[89] However, the Uganda Bankers Association (UBA) came out strongly and condemned the request as unlawful and an infringement of privacy and undermining the duty of confidentiality owed to customers by the banks. The tax body has since tactfully withdrawn from this demand. According to Section 42 of the Tax Procedures Code Act, 2014 the tax body partly has the mandate to access information about a taxpayer whenever it deems it fit, as long as it secures a court order.

Further, several Civil Society Organisations (CSOs) have come up with deliberate campaigns, programmes and activities to advocate for data protection and privacy within the public sphere. These include acquainting citizens with skills in digital literacy on the one hand and engaging policy makers and regulators on the other on the importance of data protection and privacy that upholds basic and fundamental freedoms such as the rights to expression and access to information. In addition digital security and safety trainings which are critical to equip stakeholders with the requisite skills on digital security, intellectual property, data protection and privacy, and to drive public awareness have been conducted. The media has partly helped to publicise breaches on data protection and privacy.

89 *Ismail Musa Ladu, Accessing clients' bank details: Alternatives for URA,http://www.monitor.co.ug/Business/Prosper/Accessing-clients--bank-details-Alternatives-URA/688616-4396432-c37nok/index.html*

6 Conclusion and Recommendations

6.1 Conclusion

The general awareness of data protection and privacy is low across the board. In fact, some of the probable breaches are not reported because of the low awareness surrounding issues of privacy among individuals and organisations. Additionally, the existing legal and regulatory framework facilitates infringement of privacy when compared with the established protection mechanisms. Moreover, government ministries, agencies and departments which are supposed to ensure the protection and enjoyment of privacy rights are given more powers to determine when and how the right to privacy is enjoyed. However, all is not lost as there are commendable progressive steps such as the decisions of court which seek to protect individual privacy. Similarly some law provisions guarantee individual privacy.

6.2 Recommendations

The Government should:

- Adapt international regulations such as the GDPR and best practices for local context, especially with regard to regulation of internet based companies and their interaction with local data subjects so as to protect privacy of its citizens.
- Train staff on data protection and privacy since the government handles the largest databases of personally identifiable data. This is because there have been classified document leakages perpetuated by staff who might not be aware of the ramifications.
- Lead the development of international, national and industry certifications that inspire and recognise bodies, entities, companies making the effort to achieve commendable levels of data privacy and protection. This sets them apart as trusted service providers.

Companies should:

- Train their staff on data protection and privacy since other than the government, they handle the largest databases of personally identifiable data. This is because of leakages of classified documents perpetuated by staff who might not be aware of the ramifications.
- Build competencies and institute internal processes to enhance data safety and protection while upholding user/client privacy. This includes physically securing their premises but also deploying better and updated security for their virtual operations and services.

The Media should:

- Invest in educating citizens about privacy and data protection in locally adaptable contexts. For example, health clinics might ask for information which is not vital yet the locals perceive that anything a health worker asks is permissible and unquestionable. When they understand their rights, it helps to draw out the limits, when citizens question certain things, there is proactivity from the government side.
- Exercise restraint and grace on its subjects especially if it crosses the line on privacy. This should be effectively done by double checking facts and sources of leakages of classified information.

The Academia should;

- Support civil society to lobby Governments for the development of data protection and privacy policies and enforcement of those policies through research and provision of sound evidence based research.
- Provide intellectual leadership and guidance in society through research and outreach, and highlight concerns on the right to privacy to key stakeholders, politicians and policy makers.

The Technical Community should:

- Build counter models, processes, and mechanisms to measure, monitor, report on networks that might be filtered, monitored, infiltrated by arbitrary agents who might want to steal, resale, corrupt, abuse, destroy personal data.

Civil Society should:

- Continue to lobby for adherence to fundamental rights to privacy and other attendant rights by calling the government and the private sector to order through public dialogues, capacity building, and advocacy campaigns.
- Follow the progress of draft laws, make inputs and submissions that promote fundamental human rights and promote the sanctity of freedoms and rights such as privacy, expression, information, among others.
- Engage the media in breaking down dense concepts on privacy and data protection.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, 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