Your Communication and Personal Data is Not Safe Anymore

Research Report

Your Communication and Personal Data is Not Safe Anymore

Research Report

2018

TABLE OF CONTENTS

ACKNOWLEDGEMENT

Unwanted Witness would like to acknowledge the precious contributions made by the Researchers in compiling this report. The organization is highly indebted to the respondents, especially the managers at MTN Uganda, Airtel and Africell as well as UTL. The Organization is also indebted to its Development Partners, Privacy International for their contribution in putting this report together.

Their contributions and candid remarks will be highly of invaluable use to protecting digital rights in Uganda.

INTRODUCTION

The Internet has fast become a key enabler in the exercise of the right to freedom of expression and access to information. Because of its uniqueness, it combines within one medium both the right to receive as well as the right to express and disseminate information, ideas and opinions, be it in the form of writing, or through audio or video[1].

By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole[2]

Ever since the internet was created, people have been sharing more and more of their personal information online. Although data sharing may bring benefits and has also become a necessity in peoples' interactions, it is not without risk. Personal data reveals a lot about an individual – life and thoughts. And if not protected and secured, these data can easily be exploited to harm individuals[3].

In many countries, privacy and data protection provisions exist, either within the constitutional legal frameworks or policies and remain important to help protect people's information and human rights, but they are often flouted and not adhered to[4].

As many people join the online community, they are required to share personal information from as simple as name, age, sex, to personal details including addresses and next of kin. The data is collected by different entities, including hospitals, schools, banks, employment places. Before the internet revolution, less attention was being paid to the need to protect peoples' personal data as well as ensuring their privacy – both off and online.

1 https://www.article19.org/data/files/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf
2 Ibid
3 Data Protection: Why it matters and how to protect it. https://www.accessnow.org/data-protection-matters-protect/
4 Ibid

By the nature of their core businesses, telecoms and internet service providers (ISPs) are critical in facilitating (or hindering) their clients' enjoyment of their rights to freedom of expression and privacy. This is because telecom companies and ISPs provide platforms for people to communicate, while in the process they collect vast amounts of personal data from the users of their services.

By December 2017, Uganda had an estimated amount of 19 million internet users representing 43%[5] of the total population, while mobile phone subscribers were close to 25 million.[6] Since 2012, the telecom regulator, UCC ordered mobile operators to implement a mandatory country-wide SIM card registration. Initially, mobile phone subscribers were required to register giving out detailed personal data to agencies[7] but now subscribers are required to present their national IDs for verification or Passports for foreigners. The National Identification and Registration Authority (NIRA) shared data readers with telecom companies to facilitate the process [8].

In the absence of a Data Protection and Privacy Law that would provide for the protection of the rights of the people whose data is processed, there are growing concerns on how holding agencies, such as telecom companies and others collecting and processing peoples' personal information can be held accountable.[9]

And while the major focus has been in analyzing the policies (or lack thereof) and actions of states regarding their impact on peoples' privacy and personal data as well as the general freedom of expression, not much scrutiny has been focused on these private actors and how their actions and operational procedures impact on the enjoyment of peoples' rights to privacy, personal data and general freedom of expression.

This paper therefore seeks to draw attention to the critical role that corporations, especially telecoms and ISPs play in the promotion and protection of peoples' right to freedom of expression and other human rights, including the right to privacy.

5 https://www.internetworldstats.com/africa.htm
6 https://www.ucc.co.ug/wp-content/uploads/2017/09/Quarterly-Market-Report-4Q17-V002.pdf
7 SIM card registration kicks off in March https://www.newvision.co.ug/new_vision/news/1298713/sim-card-registration-kicks-march
8 https://chimpreports.com/sim-card-registration-eased-as-ucc-receives-data-readers/
9 https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Bill%202015%20-published_0.pdf

RATIONALE AND RESEARCH GOAL

Despite the questionable legality of all the state actions and directives to the telecom companies and ISPs to limit online freedoms, and their impact on peoples' right to privacy and freedom of expression, there is little evidence that they (telecom and ISPs) have made any attempts to question or pushback these directives by the government. Nor have they engaged the users' and other stakeholders to develop mechanisms to safeguard the users' right to privacy and freedom of expression.

It is against this background that the Unwanted Witness commissioned this study to assess the existing compliance policy disclosures and practices of telecom companies and their impact on peoples' right to privacy and freedom of expression.

Specifically, the study hopes;

a) To establish existing gaps among the compliance policy disclosures and practices of four telecom companies – MTN[10], Airtel[11], Africel[12] and Uganda Telecom[13]
b) Assess the impact of these gaps on users' right to privacy and personal data protection and the wider expression and privacy
c) Provide policy recommendations to government, telecoms and other key stakeholders on how to enhance corporate accountability among telecom companies

10 https://mtn.co.ug/en/Pages/default.aspx
11 https://www.airtel.co.ug/
12 http://africell.ug/
13 http://www.utl.co.ug/

RESEARCH METHODOLOGY

The research was conducted over a period of five months, from March to July 2018 and it involved conducting a comprehensive literature review/analysis of key documents on corporate accountability and human rights, specifically on the right to freedom of expression and privacy.

These included international instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the African Charter on Civil and Political Rights, the UN Guidelines on Business and Human Rights, the Uganda Constitution, the Regulation of Interception of Communications Act, the Uganda Communications Act; as well as internal policy and guiding documents on privacy, and terms and conditions of service by the four telecom companies under review.

According to the UN Guiding Principles on Business and Human Rights[14], states are required to set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights as articulated in the national laws and policies as well as international human rights instruments, throughout their operations.

In analyzing the state's duty to protect, the study reviewed the existing legal framework and actions of the state over the last few years. In this review, the study sought to answer the following research questions, based on principle 3 of the UN guiding principles:

a) Do the existing laws and policies require business enterprises to respect human rights?
b) Do the laws and policies govern the creation and ongoing operations of business enterprise enable business to respect human rights?
c) Do the existing laws and policies provide effective guidance to business enterprises on how to respect human rights throughout their operations?
d) Do the existing laws and policies required business to communicate how they address human rights?

The UN Guidelines also require business enterprises to respect human rights by avoiding infringing on the human rights of others and should address adverse human rights impacts with which they are involved

14 http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Principle 15 requires business enterprises to have in place policies and processes appropriate to their size and circumstances, if they are to meet their responsibility in the respect for human rights, including;

In reviewing the internal policies and actions of the telecom and ISPs, the study sought to answer the following questions, developed using the Ranking Digital Rights project indicators[15]

1) If the company has policies that clearly articulate respect for users' rights including privacy and freedom of expression
2) If the company offer terms of service and privacy policies that are easy to find and easy to understand
3) If the company clearly explains the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network
4) If the company clearly discloses its process for responding to government (including judicial orders) and private requests to remove, filter, or restrict content or Accounts
5) If the company regularly publishes data about government and private requests to remove, filter, or restrict access to content or accounts

A) A policy commitment to meet their responsibility to respect human rights;
B) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;
C) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

6) If the company clearly discloses what user information it collects, why it collects, it shares the information and with whom?
7) If the company clearly discloses to users what options they have to control the company's collection, retention and use of their user information
8) If the company clearly discloses its process for responding to requests from governments and other third parties for user information
9) If the company clearly discloses information about its institutional processes to ensure the security of its products and services
10) If the company publicly discloses information about its processes for responding to data breaches

15 https://rankingdigitalrights.org/index2018/indicators/

11) If the company helps users keep their accounts secure and provides information to help them deal with cyber attacks

The research intended to collect some supplementary data through key informant interviews with officials from the four telecom companies under review – MTN, UTL, Africel and Airtel, but hit a dead end with three of them, as it was only MTN that was willing to be interviewed. This is already a negative indication, given that many of the questions to be answered consisted on how the company disclosed certain information. We hope that those three companies will participate in further studies.

The main objective for the key informant interviews was to gather relevant information that may be difficult to access due to lack of publicly available documents, specially internal policies and guidelines of the telecom companies. More efforts were made to reach out to the four companies, to get their in-put on the preliminary findings, but we still received no response, even after they acknowledged receipt of our letter requesting for feedback.

FINDINGS AND DISCUSSIONS

Weak Privacy Policies and Terms of Services by Business Entities

According to principle 13 of the UN "Protect, Respect, and Remedy" Framework and Guiding Principles, telecom companies and ISPs have a responsibility in promoting the respect for human rights by avoiding causing or contributing to adverse human rights impacts through their own activities as well as seeking to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

Terms and conditions of service including policies designed by the telecom and ISPs companies that do not comply with constitutional provisions and international human rights standards around privacy, personal data protection and freedom of expression, especially the principles of necessity and proportionality[16] pose a significant challenge in to freedom of expression in the digital age

During the research study, we conducted an analysis of the respective policies terms of services of the four telecom companies, to assess whether they provide the right to privacy and other rights such as peoples' right to freedom of expression.

Specifically, we looked at the availability of internal policies and guidelines, including terms of services that clearly prioritize customers' rights, accessibility of the same by the public/clients; existence of clear processes of how these policies are implemented in order to safeguard the rights of the clients.

No	Research questions	MTN	Airtel	Africel	UTL
1	Does the company have publicly available policies, including terms of service?	Yes	Yes	No	No
2	Does the company have policies that clearly articulate respect for users' rights including privacy and freedom of expression	No	Yes	No	No
3	Does the company offer terms of service and privacy policies that are easy to find and easy to understand	Yes	Yes	No	No

16 Article 19 (3) International Covenant on Civil and Political Rights https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

4	Does the company clearly explain the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network	No	No	No	No
5	Does the company clearly disclose its process for responding to government (including judicial orders) and private requests to remove, filter, or restrict content or Accounts	No	No	No	No
6	Does the company regularly publish data about government and private requests to remove, filter, or restrict access to content or accounts	No	No	No	No
7	Does the company clearly disclose what user information it collects, why it collects, it shares the information and with whom?	Yes	Yes	No	No
8	Does the company clearly disclose to users what options they have to control the company's collection, retention and use of their user information	No	No	No	No
9	Does the company clearly disclose its process for responding to requests from governments and other third parties for user information	No	No	No	No
10	Does the company clearly disclose information about its institutional processes to ensure the security of its products and services	No	No	No	No
11	Does the company publicly disclose information about its processes for responding to data breaches	No	No	No	No
12	Does the company help users keep their accounts secure and provides information to help them deal with cyber attacks	No	No	No	No

> *"MTN Uganda is not liable for any lack of privacy, which may be experienced with regard to the service. The Customer hereby authorises MTN Uganda to monitor and record calls made to MTN Uganda concerning the Customer's account,*

From the above table, only Airtel Uganda[17] and MTN had publically available terms and conditions of services for the different services (data, voice, mobile money,[18]among others) that they provide. These are accessible both on the hardcopy forms filled during registration as well as online. Unfortunately, these are only in English and may not be easily understood or even read by the majority of clients who sign up for the services.

Given the amount of data that telecom companies and ISPs collect and process in the course of their work, it is critical that customers' personal information and data is kept confidential and their privacy guaranteed. In the absence of a data protection law, clients are relying on the goodwill and self-made commitments from these companies to protect their privacy and confidentiality.

Of the four companies whose policies were reviewed in the research, only Airtel Uganda commits to the protection of the customers' right to privacy except under special circumstances stating that;

"Airtel will not monitor, vet, edit or knowingly disclose the contents of any emails transmitted or received by you using the Service, except that you agree that airtel may do so:

a) if required to by law;
b) if necessary to enforce any of these Terms and Conditions;
c) to respond to claims that such contents violate or infringe the rights of third-parties; or
d) to protect the rights or property of airtel[19].

17 Airtel Copyright and Privacy policy https://www.airtel.co.ug/copyRightPrivacy
18 http://beta.mtn.co.ug/Help/Legal/MTN-Mobile-Money-Consumer-Term.aspx
19 Section 7 of the Terms and Conditions for the use of airtel Data (Mobile Internet, Multimedia Messages, Portal and Blackberry) http://africa.airtel.com/wps/wcm/connect/africarevamp/uganda/3g/home/term/ accessed on 4th August 2018

This provision is also consistent with the other airtel's provision for Non Disclosure of customer's Information in their Copyright and Privacy policy, stating that;

"Due to the mutual trust with our customers, airtel will maintain at all times the privacy and confidentiality of all personal information collected. Such information may only be disclosed when required by law or when in good faith we believe that such action is necessary or desirable to comply with the law, protect or defend the rights or property of airtel, this site or its users[20]

On the other hand, MTN Uganda under their general terms and conditions of is not liable for the lack of clients' privacy when using the service, and gives itself the right to monitor and intercept and disclose any communication in order to protect itself,

"MTN Uganda is not liable for any lack of privacy, which may be experienced with regard to the service. The Customer hereby authorises MTN Uganda to monitor and record calls made to MTN Uganda concerning the Customer's account, or the service and the Customer further consents to the use by MTN Uganda of automatic dialing equipment to contact the Customer. MTN Uganda has the right to intercept and disclose transmissions over the MTN Uganda facilities, in order to protect MTN Uganda's rights and property."[21]

This provision contradicts the MTN's privacy policy[22] provisions which commits to the protection of their customers private information and confidentiality stating that:

"we will not make your personal information available to anyone unless permitted or required to do so by law. We will therefore not sell, rent or provide your personal information to unauthorised entities or third parties for their independent use without your consent. We may, however, share your personal information with our affiliates within the MTN Group of companies." [23]

For both companies, they emphasise that these policies as well as the terms and conditions of services are governed by the laws of Uganda and UCC regulations. This could explain the reluctance to pushback directives from the state for fear of losing their licenses, but that does not mean that companies should assume that they should honour any government request, and much less so when constitutional rights are at stake.

20 Airtel Copyright and Privacy policy https://www.airtel.co.ug/copyRightPrivacy accessed on 4th August 2018

21 Section 6(a) of the General Terms and Conditions of Internet Service Provision http://beta.mtn.co.ug/Help/Legal/Terms-and-Conditions-for-Inter.aspx accessed on 4th August 2018

22 MTN Privacy Policy https://www.mtn.co.ug/en/Pages/privacy-policy.aspx accessed on 4th August 2018

23 Ibid Section 5: Protection of Personal Information

Weak and Fragmented National Policy and Regulatory Framework

As the primary duty bearer for protecting and promoting human rights, the Uganda government has the responsibility of ensuring that the prevailing legal and policy frameworks are watertight and not exploitable by the telecom companies operating within its jurisdiction to commit human rights abuses.

Although Uganda's 1995 Constitution (as amended) provides for the rights to freedom of expression (Article 29(a); including that of the media, the right of access to information (Article 41), and the right to privacy (Article 27), subsequent legislation often times makes it difficult or impossible for companies to fulfill to respect human rights online by imposing legal and regulatory frameworks that are incompatible with the right to freedom of expression as defined under international human rights law.

The Anti-Terrorism Act (2002)[24] gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance. The scope of the interception and surveillance includes letters and postal packages, telephone calls, faxes, emails and other communications, access to bank accounts, as well as monitoring meetings of any group of persons[25].

The Regulation of Interception of Communications Act (RICA) 2010[26] under section 5 gives the government permission to tap into personal communications for national security concerns, which can be requested by the security minister and granted after an order by a High Court judge. Additionally, section 11 requires service providers are further required to retain metadata for an unspecified amount of time, as well as disclose the personal information of individuals suspected of terrorism to the authorities upon issuance of a court warrant or notice from the security minister on matters related to national security, national economic interests, and public safety (section 8). Failure to comply with the provisions in the RIC Act can entail penalties of up to five years in prison for intermediaries, in addition to license revocations

24 https://ulii.org/ug/legislation/act/2017/4

25 CIPESA (2014) The State of Internet Freedom in East Africa, https://www.cipesa.org/?wpfb_dl=76

26 http://www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

The Uganda Communications Commission Amendment Bill 2016[27], effectively expunged parliamentary oversight on the regulations made by the minister. In the amended law, the phrase "with approval of parliament" was removed from section 93(1) of the Act[28] which read;

"The Minister may, after consultation with the Authority and with the approval of Parliament, by statutory instrument, make regulations for better carrying into effect the provisions of this Act.". The strengthened power of the minister was witnessed when he ignored parliament's motion to extend SIM card re-registration and instead directed the UCC to switch off all unverified cards in May 2017[29]

But even without the amendment, the Act already gives sweeping powers to the minister as well as UCC to regulate, monitor and to conduct communication surveillance of citizens' communications across all communications/ expression platforms including the internet[30].

The net effect of these retrogressive legal frameworks is that they can easily be abused by the state and business entities, such as telecom companies and ISPs for their own benefit. A number of telecom companies have been accused by users of "selling" their details and allowing junk messages. In 2014, MTN was sued for unsolicited electronic messages.[31] In an evaluation report of MTN performance over the last 20 years by UCC, the telecom giant was found to failed to comply with the regulatory directive to stop forthwith sending unsolicited electronic messages without the "opt out" option to users.[32]

Around May 2018, it took a twitter storm to compel the regulator, UCC to direct MTN to review its Mobile Money policies to make it easier for clients who send money in error to compel the recipient to send back the money.[33]

27 http://www.chimpreports.com/parliament-passes-communications-amendment-bill/
28 http://chapterfouruganda.com/sites/default/files/downloads/The-Uganda-Communications-Amendment-Bill-2016.pdf
29 https://freedomhouse.org/report/freedom-net/2017/uganda
30 https://www.unwantedwitness.or.ug/internet-they-are-coming-for-it-too.pdf
31 https://www.observer.ug/news-headlines/33285--mtn-sued-over-junk-bulk-sms-
32 https://www.ucc.co.ug/wp-content/uploads/2018/03/ucc_evaluation_report_on_MTN_Uganda_march_2018.pdf
33 http://www.theeastafrican.co.ke/business/Uganda-to-probe-MTN-on-mobile-money-policies/2560-4587696-vhm83n/index.html

Increase in State Directives to Telecoms and ISPs

Over the last 10 years, the state has made several attempts, requesting and ordering telecom companies and ISPs to censure, block or intercept online communications, as well as mobile money transactions.

In April 2011, the regulator – the (UCC) – instructed ISPs to block access to Facebook and Twitter for 24 hours "to eliminate the connection and sharing of information that incites the public." The order came in the heat of the 'walk to work' protests in various towns over rising fuel and food prices.

The letter from the regulator stated that the order had been prompted by "a request from the security agencies that there is need to minimise the use of the media that may escalate violence to the public in respect of the on-going situation due to the demonstration relating to 'Walk to Work', mainly by the opposition in the country."

During the elections in February 2016, the government banned social media on Election Day with the president defending the decision as a "security measure."[34] Unfortunately, the practice continued during the swearing in ceremony in May 2016, when once again social media platforms were blocked[35]. The impact had however been massive as majority of people who rely on the mobile money platforms to transact their business were affected[36], and those who rely on social media for information were also affected.

In November 2016, security agents arrested journalist Joy Doreen Biira on charges of "illegal filming of military raid" on a regional king's palace, which resulted in civilian deaths. In a crude act of censorship, both Gertrude Uwitware and Joy Biira were forced to remove their respective offending posts from social media[37]

34 http://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/
35 http://allafrica.com/stories/201605130317.html
36 http://www.cgap.org/blog/impact-shutting-down-mobile-money-uganda
37 Freedom on the Net 2017 Uganda https://freedomhouse.org/report/freedom-net/2017/uganda

As recent as July 2018, there were disturbing reports of a raid on the data center of one of the telecom giants in Uganda, MTN Uganda by alleged security agents, who tampered with clients' personal data.[38] According to a letter written to the Director of the Uganda's Internal Security Organisation (ISO), as quoted by the East African newspaper[39], the telco said security men alleging to be from the agency in charge of domestic intelligence intruded into the data centre on July 2.

The Telecom company alleges in its letter that the men kidnapped an employee of its contractor -- Moses Keefah Musasizi, a data manager for Huawei Uganda, who is responsible for access into the firm's data centre. In the letter, MTN said Mr Musasizi was abducted at 5pm local time and taken to the ISO head office in Nakasero, some 9km northeast away. He was held there until 9pm when he was returned to the data centre and forced to give access to the security men. He was also ordered to disconnect the four servers, MTN adds. "We are yet to determine the extent of interruption to our network activities and the financial impact. It is also possible that some data have been tempered with or illegally accessed and taken from the premise," the letter reads, as quoted by the East African newspaper.

In March 2018, the communication regulator, UCC directed Internet Service Providers to suspend the provision of carriage services to any online data communication service providers that has not been cleared by the regulator to provide such services in the country. In its letter, UCC listed a number of providers that had been cleared at the time and those whose application it was considering.

38 https://www.reuters.com/article/us-uganda-mtn-group/mtn-uganda-says-government-security-personnel-raided-its-data-center-idUSKBN1JW1Q5

39 http://www.theeastafrican.co.ke/business/MTN-Uganda-data-centre-raided/2560-4650068-y6styoz/index.html

UGANDA COMMUNICATIONS COMMISSION

Head Offices: UCC House, Plot 42-44 Spring Road, Bugolobi
P.O. Box 7376 Kampala - UGANDA
Tel: +256 41 4339 000, +256 31 2339 000
Email: ucc@ucc.co.ug
Toll Free Line: 0800133911
Website: www.ucc.co.ug

Our Ref: LA/548

19th April 2018

All Internet Service Providers (ISPs)

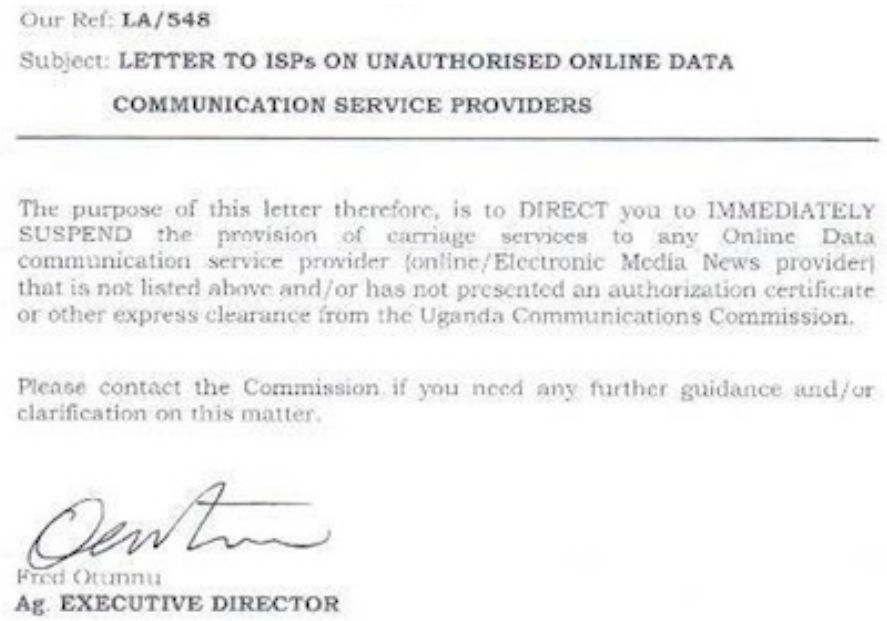
RE: UNAUTHORISED ONLINE DATA COMMUNICATION SERVICE PROVIDER

Reference is made to the above subject matter and a public notice issued by the Uganda Communications Commission (Commission) on the 6th March 2018 requiring all Online Data Communication Service Providers (online newspaper service providers) to apply and obtain authorization from the Commission.

This is to confirm that the following providers have applied for and the Commission is considering their applications for authorisation to provide Online Data Communication Services in Uganda;

S/N	Name of Service Provider	Status
1.	Nile Post News Uganda Ltd	Authorised
2.	China Haijiang Online Africa Ltd	Authorised
3.	Dimension Media Ltd	Application in process
4.	Post Media Ltd	Application in process
5.	Uganda Online Website Directory	Application in process
6.	Hive Digital Ltd	Application in process
7.	Mirror Digital Ltd	Application in process
8.	Trumpet Media Ltd	Application in process
9.	Newslex Point Ltd	Application in process
10.	Gold Cast (U)Ltd	Application in process
11.	Newscom Uganda Ltd	Application in process
12.	Hot Spot Ltd	Application in process
13.	Chimp Media Ltd	Application in process
14.	Guide 2 Uganda	Application in process

1998-2018



Our Ref: **LA/548**

Subject: **LETTER TO ISPs ON UNAUTHORISED ONLINE DATA COMMUNICATION SERVICE PROVIDERS**

The purpose of this letter therefore, is to DIRECT you to IMMEDIATELY SUSPEND the provision of carriage services to any Online Data communication service provider (online/Electronic Media News provider) that is not listed above and/or has not presented an authorization certificate or other express clearance from the Uganda Communications Commission.

Please contact the Commission if you need any further guidance and/or clarification on this matter.

Fred Otunnu
Ag. EXECUTIVE DIRECTOR

communication providers, including online publishers, online news platforms, as well as online radio and television operators to apply and get authorization from the UCC with immediate effect.

Implementing State Directives to the Letter

According to the UN "Protect, Respect, and Remedy" Framework and Guiding Principles, the corporate responsibility to respect human rights means acting with due diligence to avoid infringing on the rights of others, and addressing harms that do occur[40]

Although section 79 of the UCC Act 2013 bars telecom operators and ISPs or their employees from intercepting or unlawfully disclosing communication between persons that they (operator or employee) are aware of, telecom companies and ISPs have been too eager to implement government directives without questions.

40 https://www.business-humanrights.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

During the 2016 presidential and parliamentary elections, most Ugandans were denied their right to freedom of expression and access to information by the actions of the telecom companies and ISPs after the two implemented a government directive to shut down internet and mobile money services.

According to Mr. Anthony Katamba, the General Manager Corporate Services at MTN Uganda, they receive directives from "government" from time to time to restrict online communication and that the regulator has the powers to make such directives "and we have always complied"[41].

Effective July 1st, 2018, the government introduced a new tax on social media that is called over the top (OTT) and a 1% levy on Mobile Money transactions, and directed telecom companies to deny services to any client who will not have paid a daily fee of UGX 200. In a joint statement, the telecom companies MTN, Bharti Airtel and Africell, said that OTT services can only be accessed on payment of the OTT tax by the customer[42].

Below is a statement that the telecoms issued regarding the tax that the government had imposed on OTT services. While it could be argued that the telecoms and other ISPs were implementing a government directive, at no point had they offered any intervention during the drafting and debate of the bill before parliament.

41 Interview with Mr. Anthony Katamba – July 15th 2018

42 https://af.reuters.com/article/ugandaNews/idAFL8N1TV3TZ

PUBLIC NOTICE: **OTT TAX**

Following the directive from the Government of Uganda, a new tax is to be implemented on Over The Top (OTT) services effective 1st July, 2018.

We hereby inform the general public of the introduction of the new taxes on the OTT services.

OTT services are applications that offer voice and messaging over the Internet; for example, but not limited to: Facebook, WhatsApp, Twitter, SnapChat, Instagram, Skype, Linkedin etc.

Effective 1st July, 2018; OTT services can be accessed upon payment of the OTT Tax by the customer of Ushs 200 per user, per day.

Payment of the OTT Tax can be made by the customer using their Mobile Wallet, EVC or any electronic wallets upon which access to the OTT services will be granted.

- MTN Mobile Money **(*165*2*8#)**
- Airtel Money **(*185*2*5#)**
- Africell Money **(*144*2*5#)** or Africell EVC **(*133*6#)**

Africell customers can also pay this tax using MTN Mobile Money or Airtel Money at no extra charge.

Access will be granted for a calendar day i.e. from the moment of payment until 11:59 PM of that same day. For the convenience of customers we have the following options:

- Daily (Ushs. 200),
- Weekly (Ushs. 1,400)
- Monthly (Ushs. 6,000)

Should you have any questions or queries regarding the above, please contact us on the Customer Toll Free line 100 or visit our websites.

airtel THE SMARTPHONE NETWORK MTN africell

CONCLUSION

The existing legal framework is at best contradictory but is quite retrogressive and doesn't provide a succinct framework to telecom companies and ISPs to promote and protect users' rights privacy, personal data protection as well as freedom of expression. As such, the telecom companies have not provided and challenge, legal or otherwise to state directives to shutdown online platforms, including sharing of users' personal data.

The lack of a data protection and privacy that provides principles and guideline for data curators on how to collect, process and share peoples' personal data provides fertile grounds for both the state and corporate agencies to undermine peoples' right to freedom of expression and the right to privacy, without any limitations.

Additionally, the four telecom companies, MTN, Airtel, Africell and UTL do not have watertight policy and terms of service that provide for the respect of human rights, including the right to privacy, personal data and freedom of expression. Those that have such as MTN and Airtel, the policies and terms of service are only in English and not easily accessible unless a user logs onto their websites. Our efforts to engage them on their existing mechanisms in protection of users' right to privacy and protection of personal data did not yield much as only MTN responded to our initial request for interviews.

RECOMMENDATIONS

For the State:

- Approve a data protection law, with an independent body that enables its enforcement to protect people's rights.
- Refrain of making illegal requests to telecommunications companies, acting only within their legal powers and respecting the Constitution and Human Rights obligations of the country.

For telecommunications companies:

- Develop terms of use, privacy and data protection policies that are in an accessible manner and falls in line with their obligations of protecting their users' human rights.
- Periodically issue transparency reports, featuring state requests of data, communications interception, blocking and other similar requests, alongside with the company response to those requests.
- Improve their digital security standards and notify their users of any security incident that could affect their rights and freedoms.
- Engage NGOs and networks that include marginalized and at-risk individuals and communities who have different experiences and interactions with the private sector with regard to freedom of expression.
- Pursuing strategic litigation against legal and policy provisions that provide for telecom companies to infringe on peoples' online freedoms.

For civil society and human rights defenders:

- Conduct more research on the impact on freedom of expression and right to privacy resulting from actions and procedures of corporate companies, especially telecoms and ISPs and communicate those findings to International bodies, the State, and the private sector.
- Support private sector in pushing back against government attempts to undermine human rights such as privacy and freedom of expression.

- Advocate for the review and strengthen of the privacy policies and terms of service in the private sector to clearly provide for the respect for human rights.

Appendix: Interview Questions with Telecom Companies
Dear Sir/Madam,

My name is_____

I am conducting a survey on behalf of the Unwanted Witness about the role of telecom companies in the promotion and protection of human rights, specifically, the right to freedom of expression and privacy.

As telecom companies, you are central to facilitating the enjoyment of peoples' right to freedom of expression, and you are also critical players in in ensuring peoples' right to privacy given the amount of personal data that you collect in the process of providing the services to the people (voice, data).

1) As (MTN/Airtel/UTL/Africel), how do you ensure that Ugandans are enjoying their full rights to freedom of expression and yet at the same time protect their privacy?
2) Do you have publicly available policy regarding user's rights to privacy and data protection? (probe: how does the public get access to them and how easy to read and understand are they?)
3) Has your company ever received any orders to restrict online communication from the government or anybody else? If yes, how did you deal with them without compromising the rights of your clients/users)
4) Do you ever publish these requests as a form of accountability to your clients/users?
5) How do you deal with private requests for removal, filtering of restrictions of your clients' accounts?
6) In situations where the government requests access to a user's private data, do you notify the user?
7) As an institution, do you provide users with the tools to keep their data safe and secure?
8) Any last comments?

Thanks for your time.

Block 381, Plot No. 26, Nsibambi village
P.O.Box 71314 Clock Tower K'la
Tel: +256 414 697635
Email: info@unwantedwitness.or.ug
Website: www.unwantedwitness.or.ug
Unwantedwitness-Uganda
@unwantedwitness
unwantedwitness