
# Intermediary Liability in Uganda

by Ashnah Kalemera, Lillian Nalwoga and Wairagala Wakabi

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

*Intermediary Liability in Africa Research Papers No. 5*

*Independent research commissioned by the Association for Progressive Communications and supported by Google Africa*

# Table of Contents

## Introduction

Uganda has an estimated population of 34.1 million with a teledensity (fixed and mobile) of 52.1 and 48 mobile subscribers per 100 inhabitants.[1] According to the regulator, the Uganda Communications Commission (UCC), the entry of new service providers and increased capacity investment in broadband by operators has resulted in increased internet penetration and changes in the methods of access. Most Ugandans access the internet on their mobile phones. With 977,500 mobile and 88,786 fixed internet subscribers and the cost of bandwidth coming down, the numbers are bound to continue growing in the coming years. According to UCC, there were approximately 4.8 million internet users in Uganda, or 14% of the population as of December 2011.[2]

Fixed internet subscriptions are mainly from home, schools, work and cyber cafes, - where it costs less than one USD for an hour's browsing. Also, with mobile internet access becoming cheaper,[3] a growing number of Ugandans are able to use cellphones and other internet-enabled devices to access social networks, news sites, and other websites at a reasonable cost. A mobile internet package through MTN Uganda, the provider with the largest number of subscribers, costs Shs500 (USD 0.20) for 10MB of data and Shs15, 000 (USD 6) for 300MB of data.[4] Free access to Facebook and Wikipedia is available to MTN and Orange mobile network subscribers, although the free service limits what a user can do. Modem costs range between US$24 and US$41. A monthly limited internet package of 1GB costs US$18 while an unlimited broadband internet connection from Orange Uganda costs US$124 for one month and up to US$673 for six months.

Since the liberalisation of the telecommunications sector in 1998, the number of players in each segment has grown, and many now offer almost the same prices and technologies, with the bigger well-established telecom operators enjoying a lion's share and having powers to dictate prices. As of April 2012, the UCC reported 17 licensed and operational internet service providers.[5] Feeble attempts at interconnection regimes regulation by UCC[6] and the poor infrastructure sharing culture among telecommunications operator also represent barriers to entry, as do licence fees.

Under the Telecommunications (Licensing) Regulations, 2005[7] the UCC issues two types of licenses: a Public Service Provider[8] (PSP) license which allows operators to set up their own

[1] Uganda Bureau of Statistics, 2012 Statistical Abstract, http://www.ubos.org/onlinefiles/uploads/ubos/pdf%20documents/2012StatisticalAbstract.pdf; International Telecommunications Union, http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#

[2] Uganda Communications Commission (UCC), 2011/2012 Post and Telecommunications Market Review, http://www.ucc.co.ug/images/stories/2011-12%20Half%20Year%20Market%20Performance%20Review.pdf

[3] "Ugandan telcos lower mobile Internet tariffs," IT News Africa, April 17, 2010, http://www.itnewsafrica.com/2010/04/ugandan-telcos-lower-mobile-internet-tariffs/.

[4] "MTN Mobile Internet," http://mtn.co.ug/MTN-Internet/MTN-Mobile-Internet.aspx.

[5] UCC, Telecommunications Licences as of April 2012, http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=53&Itemid=56

[6] On January 7, 2005, the Telecommunications (Interconnection) Regulations came into effect, and aimed to "establish an effective and competitive framework for regulating the interconnection and interoperability of telecommunications networks and systems, infrastructure facilities and services through measures." Over the years, there have been concerns that while UCC was mandated to regulate interconnection rates, it hardly acted proactively nor had it tried to protect consumers' rights in its work on the issue of interconnection. The regulator allowed operators to enter into commercial agreements (negotiated, cost-based or otherwise) with other operators with regard to termination rates and only intervened when disputes arose.

[7] UCC, The Telecomunications (Licencing) Regulations, 2005, http://www.ucc.co.ug/files/downloads/licensingRegulations.pdf

[8] For PSP, two types of licences are issued: (1) Public Voice and Data Licence: this permits holders to provide voice and data services of any kind (fixed, mobile or both) using technologies of their choice (cellular, satellite, internet protocol, wired networks). A holder of this licence must use the capacity and facilities of a PIP, or build

infrastructure or use the capacity and facilities of a Public Infrastructure Provider (PIP) which is licensed to establish, operate and maintain infrastructure for the provision of communications services.

PIP licence holders establish, operate and maintain infrastructure for the provision of communication services as a PSP licence holders and/or commercially to third parties. A holder of either of these licenses can be considered an internet intermediary.[9]

Applications fees are USD 2,500 (PSP) with a one-off initial fee of USD100,000 for a PIP license. Operators are further charged an annual fee of USD 3,000-10,000 and a 1% levy of gross annual revenue.[10] In line with recent developments in the industry, the regulator has undertaken a review of the interconnection, pricing and competition regulatory frameworks.

Over recent years, issues regarding intermediaries have been restricted to the disclosure of user information/ data in law enforcement and screening, filtering or blocking certain information. The constitution of Uganda provides for freedom of expression and press freedom. In general, there are no restrictions to internet access in Uganda. However, there have been government crackdowns on critical journalists both in online and print media. Also, there have been reported cases of online censorship and the charging of a journalist over a story published online.

This paper reviews the state of intermediary liability in Uganda. In particular, it explores regulations relevant to the responsibilities of intermediaries. It cites incidences of content takedowns, attempts to block access to internet content, mobile content filtering and media persecutions, and the applicable sections of the law.

their own infrastructure upon receiving a PIP licence. (2) Capacity Resale Licence: the holder of this licence is allowed to resale leased or bought telecommunications services or capacity. This includes calling cards and telecommunications bandwidth to PSPs.

[9] UCC Telecommunications Licences as at April 2012, http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=66&Itemid=66

[10] and Application Procedure http://www.ucc.co.ug/licensing/procedure.php

## Legislative, Policy and Regulatory Environment

Provisions in a number of Ugandan legislations contain similar terms to 'internet intermediaries' that are relevant to intermediary liability. However, Uganda has no legislation that explicitly provides for the liability of "intermediaries" in filtering, removing or blocking content considered objectionable. Current legislation such as The Communications Act of 2000 (Cap 106)[11], The Regulation of Interception of Communications 2010[12], Electronic Transactions Act (No 8 of 2011)[13] and the Uganda Communications Regulatory Authority Bill of 2012[14] broadly encompass intermediaries in their interpretations of telecommunications entities. In their preliminary clauses, the three legislations describe telecommunications entities as those providing *"services consisting of the conveyance or reception of any sound, signs, signals, writing or images by wire, optical or other electronically guided media systems whether or not the signs, signals, writing, images, sounds or intelligence have been subjected to re-arrangement, computation or other process by any means in the course of their transmission, emission or reception."* [15] Current legislation does not differentiate between fixed and mobile internet intermediary liability. Mobile operators seem to have received the bulk of the focus regarding liability; there have been incidents (mentioned below) where mobile operators have been asked to block or filter content.

**The Anti Terrorism Act No.14** of 2002 states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism is also liable be sentenced to capital punishment upon conviction. The law gives the Minister for Internal Affairs power to dissolve any terrorist organisation, provide for its closing down, and for the forfeiture to the state of its assets.

Moreover, the Act gives security officers powers to intercept the communications of a person and to keep such persons under surveillance. The scope of the interception and surveillance specified by the law include interception of letters and postal packages of any person; interception of telephone calls, faxes, emails and other communications made or issued by or addressed to a person; and monitoring meetings of any group of persons. Others powers include the surveillance of the movements and activities of any person; electronic surveillance of any person; access to bank accounts of any person; and searching of the premises of any person. The Act says that the purposes for which interception or surveillance may be conducted are for the safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism.

Any person who obstructs terrorism investigations, interception of communications and surveillance under the Terrorism Act commits an offense and is liable on conviction, to imprisonment not exceeding two years or a fine, or both. This potentially exposes intermediaries for liability for not cooperating with authorities.

---

[11] Uganda Communications Act (2000), http://www.ulii.org/ug/legislation/consolidated-act/106

[12] Parliament of Uganda, http://www.parliament.go.ug/new/index.php/parliamentary-business/bills

[13] Electronic Transactions Act, 2011, Ministry of Information and Communication Technology, http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=59&Itemid=61

[14] The Uganda Communications Regulatory Authority Bill available at http://www.acme-ug.org/media-laws/doc_details/93-uganda-communications-regulatory-authority-bill-2012 it has recently been passed into law but not yet assented to by the president.

[15] Uganda Communications Act, Part I, Section 1; Regulation of Interception of Communications, Part I, Section 1; and Electronic Transactions Act, Part I, Section 2.

The Regulation of Interception of Communications (RIC) Act 2010 allows for interception of communications and possible intrusion into personal communications.[16] The Act requires telecommunications companies to collect customer information including name, address, identity number as contained in his or her identity document and "any other information which the telecommunication service provider deems necessary" for the purpose of enabling it to comply with the Act.[17] Furthermore, to install electronic surveillance and interception equipment that "identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment facility or service provided by a service provider and, where applicable, the location of the user within the telecommunications system".[18] Telecommunications service providers are obliged to disclose information of customers on "reasonable cause" to suspect terrorism to authorities. The disclosure requirements are upon issue of a warrant by court or notice of disclosure by the minister on matters relating to national security, national economic interest and public safety. Furthermore, Part II sections 2 and 3 of the RIC Act 2010 gives the government permission to monitor the personal communications of persons that are a potential threat to national security. This legislation also covers postal service providers.

Intermediaries are responsible for monitoring network traffic under the RIC. They are obliged in section 8 of the Act to provide assistance to the "monitoring centre" – a state security agency authorised to effect interceptions by ensuring that their services can render real time and full time monitoring facilities for interceptions. In addition, they have to offer all call-related information for a person under surveillance in real-time or soon after call termination:

Where a service provider fails to give assistance to the monitoring centre under the above section, the entity commits an offence and upon conviction is liable to a fine or imprisonment for the responsible persons for a period not exceeding five years. No minimum sentence period is stipulated in the act. Furthermore, the intermediary's operating license may be cancelled.

**The Electronic Transactions Act (2011)** defines an "intermediary" as "a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message."[19] On the other hand, it describes a service provider as "any public or private entity that provides to the users of its service the ability to communicate by means of a computer system", and "any other entity that processes or stores computer data on behalf of such communication service or users of such service".[20] Section 4 of the same Act provides a framework to among others, enable and facilitate electronic communication and transactions; promote technology neutrality in applying legislation to electronic communications and transactions; and provide legal certainty and public confidence in the use of electronic communications and transactions.

Section 29 of the Electronic Transactions Act delineates the liability of service providers. It states that a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access. This is provided that the intermediary is not directly involved in the making, publication, dissemination or distribution of the material or a statement made in the material; or the infringement of any

[16] Regulation of Interception of Communications (RIC) Act 2010 – (Part III: Sections 9,10 and 11)
[17] Section III, Part 9
[18] Ibid
[19] Part I, Section 2
[20] Part I, Section 2

rights subsisting in or in relation to the material. The Act, however, states that the above section does not affect the obligations of a service provider under a licensing or regulatory framework established by the law, or any obligations imposed by law or a court to remove, block or deny access to any material.

In section 29, providing access in relation to third-party material, is defined as "providing the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access." The Act defines a third party as a "subscriber to a service provided by the service provider or any other user of the service provider's services or a user of information systems."[21]

The Act further in Section 30 states that service providers are not liable for infringement for referring or linking to a "data message or infringing activity" if the service provider:

- does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;
- is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
- does not receive a financial benefit directly attributable to the infringing activity; or
- removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

Persons with complaints about a data message or related activity are required to notify the service provider or his or her designated agent in writing giving details of the right allegedly infringed and remedial action required to be taken by the service provider in respect of the complaint. However, this legislation is silent on what happens in case the service provider does not comply, or the appeal mechanisms the party accused of infringement may take.

Section 32 of the Electronic Transactions Act does not require service providers to monitor stored or transmitted data nor "actively seek for facts or circumstances indicating an unlawful activity."

The Uganda telecommunications sector regulator, UCC, was established under the **Communications Act (2000).** It is an independent statutory body mandated to coordinate, facilitate and promote the sustainable growth and development of Uganda's communications sector. The Commission has the power to "on occurrence of any state of emergency or in the interest of public safety direct any operator to operate networks in such a manner as is appropriate to alleviate the state of emergency."[22] Part XVII, Section 90, of the Communications Act also gives UCC the power to (in case of a state of emergency or in the interest of public safety) *"take temporary possession of any communications station within Uganda, and any apparatus which may be installed and used in the station, for a period not exceeding six months" and "in writing to a licensed person, direct that a postal article, or class or description of postal articles in the course of transmission within Uganda be intercepted or detained or be delivered to any officer mentioned in the order to be disposed of in a manner specified by the commission."* An operator is

[21] Part I, Section 2
[22] Part XVII, Section 90

defined as "any licensee" providing services consisting of the dissemination or interchange of sound, video or data content using postal, radio or telecommunications media.

The Commission is funded through operator licence fees, an annual levy on operator profits, government budget allocations and "loans, grants, gifts or donations from the Government and other sources, acceptable to the Minister and the Minister responsible for finance with the approval of Parliament"[23] . Nonetheless, the commission is mandated to exercise its powers independently under Part II Section 12 of the Act.

In March 2012, the Ministry of ICT proposed the Uganda Communications Regulatory Authority Bill (2012). The bill, which seeks to amend the Electronic Media Act 1997 and the Communications Act 2000, is aimed at controlling and regulating broadcasting, telecommunications and postal services. The establishment of the Uganda Communications Regulatory Authority under the bill seeks to among other goals, monitor, inspect, license, supervise, control and regulate communications services. The new authority would entail a merger of UCC and the Uganda Broadcasting Council. The Bill guards against infringing the privacy of persons and dissemination of false information. In addition, it prohibits broadcasting (the transmission of sound, video and data) programmes contrary to public morality and denounces distortion of facts and unbalanced information "regardless of the technology". The bill only outlines offences related to unlicensed operators, fraud, equipment, unlawful interception and false advertising. Part XIV, Section 92 mentions a "general penalty" fine for any person convicted of an offence under the Act for which no minimum or maximum sentence is provided.

The proposed law maintains the clause from the RIC Act on telecommunications service providers' obligations to install surveillance equipment and collect and maintain records of their customers, and to disclose this information to authorities if based upon a "reasonable ground". Internet intermediaries are again broadly covered under definitions of telecommunications service providers.

Uganda is not a signatory to any known international agreements on intermediary liability but a state party to the World Trade Organization (WTO) agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (1994). The Copyright and Neighbouring Rights[24] Act 2006[25] which repealed and replaced the Copyright Act Cap 215, provides for the protection of literary, scientific and artistic intellectual works and their neighbouring rights. Section 46 of the Act states that infringement of copyright or neighbouring right occurs where, "without a valid transfer, licence, assignment or other authorization" a person deals with any work or performance contrary to the permitted free use and in particular where that person does or causes or permits another person to:

- reproduce, fix, duplicate, extract, imitate or import into Uganda otherwise than for his or her own private use;
- distribute in Uganda by way of sale, hire, rental or lsimilar manner; or

[23] Uganda Communications Act, 2000: Part IV Section 1,

[24] Neighbouring Rights, also known as Related Rights extend copyright of an original work to protect the legal interests of performers, producers and broadcasters who contribute to making works available to the public. "The law of related rights deems that productions which result from the activities of such persons and entities merit legal protection in themselves, as they are related to the protection of works of authorship under copyright." World Intellectual Property (WPO), Understanding Copyright and Related Rights, http://www.wipo.int/freepublications/en/intproperty/909/wipo_pub_909.html#rights

[25] Uganda, The Copy Right and Neighbouring Rights Act 2006, http://www.wipo.int/wipolex/en/text.jsp?file_id=141975

- exhibit to the public for commercial purposes by way of broadcast, public performance or otherwise.

Among the copyright offences in Section 48 of the Act are the publication, distribution, broadcasting and communication to the public of copyrighted work including via the internet. A person who commits an offence is liable on conviction, to a fine or imprisonment not exceeding four years or both.

Private sector industry associations do not play a large role in advocacy around issues affecting intermediaries. In the past, there was an industry association of Internet Service Providers (ISPs) in Uganda - the Uganda Internet Service Providers Association (UISPA). Over the years it played some roles in the sector, such as enabling numerous ISPs to buy bandwidth in bulk so as to retail it at lower prices, and making presentations to the government on issues of concern to ISPs. The association is now inactive, primarily because its main promoter has divested most of his interests in internet service provision. But even at when the UISPA was most vibrant about four years ago, it was not engaged in advocacy around intermediary liability. Intermediaries do not seem to be to interested in advocating for procedures that would protect the rights of third parties which may have their content subject to takedowns. One practitioner, who preferred anonymity, stated that *"unfortunately no business person (hosting business) is going to risk their business on principle so take-down is here to stay. In fact it is practiced in the U.S. so many times a day it is a way of life and most times not even reported. It only takes a letter from a lawyer for take-down to happen [in Uganda]."* The nation's civil society organisations and ICT fraternity are also not active in issues around intermediary liability or the takedown of content.

## Cases involving takedowns or intermediary liability in the past five years

Intermediaries in Uganda monitor user behaviour according to legislative and regulatory frameworks such as the RIC Act, 2010 and Communications Act, 2000. Although the legislation in Uganda clearly states the circumstances under which an order may be made for content to be taken down or blocked on terrorism or other grounds, recent years have seen instances of takedowns that have infringed on the rights to freedom of expression and opinion and freedoms of association and assembly. There have been orders to takedown or block access to certain websites, with at least one court case against an online journalist as explained in the sections below:

**Attempts to block access to Facebook, twitter:** On April 14, 2011, the regulator – the Uganda Communications Commission (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." At the time, UCC executive director Godfrey Mutabazi told Reporters Without Borders that he would again order that access to Facebook and Twitter be cut off if it had to be done to protect the public. "The freedom to live is more important than the freedom to express oneself," said the regulator, explaining that he was only appealing to Ugandans to take care not to use social networks to issue calls for hatred or violence.[26] Some ISPS said they did not comply with the order, having received it after the 24-hour period during which the regulator had ordered them to block access although this could not be independently verified.

Filtering and blocking of Text Messages: Earlier in February 2011, UCC directed telecom companies to block and regulate text messages that could instigate hatred, violence and unrest during the presidential election period. A report in the Daily Monitor said the Communications Commission had released 18 words and names which mobile phone short message service (SMS) were instructed to flag if they were contained in any text message. They were then supposed to read the rest of the content of the message and if it was deemed to be "controversial or advanced to incite the public", it would have to be blocked. The words included 'Tunisia', 'Egypt', 'Ben Ali', 'Mubarak', 'dictator', 'teargas', *'kafu'* (it is dead), *'yakabbadda'* (he/she cried long time ago), *'emuudu/emundu'* (gun), *'gasiya'* (rubbish), 'army/ police/UPDF', 'people power', and 'gun/bullet'. Two UCC spokesmen confirmed this report, saying the aim was "to ensure free, fair and peaceful elections".[27] It was not clear whether the intermediaries actually complied with this directive.

According to *Daily Monitor*, the letter from the UCC executive director read: "Messages containing such words when encountered, by the network of facility owner or operator, should be scrutinised and if deemed to be controversial or advanced to incite the public should be stopped or blocked. A report of all blocked messages should then be prepared and submitted to UCC in 48 hours." It could not be established whether any such reports were submitted.

[26] RSF, government could target Facebook and twitter on eve of new protests, April 20, 2011; http://en.rsf.org/uganda-government-could-target-facebook-20-04-2011,40068.html

[27] Benon Herbert Oluka, Uganda to intercept text messages, Daily Monitor, February 18 2011

The opposition party Forum for Democratic Change (FDC) alleged in 2011 that the phone company MTN had sabotaged its presidential elections results tally centre by jamming the telephone lines of its polling station agents, thereby making it impossible for them to transmit results. During the elections, the party set up its own tally centre but ultimately its results were released nearly two weeks after the official declaration of the election results. The party called for a boycott of MTN services, which has the biggest number of subscribers of all operators in Uganda.[28]

**Online journalist charged:** Timothy Kalyegira, editor of the online newspaper Uganda Record was in July 2010 charged with publishing material online "with intent to defame the person of the President". The prosecution alleges that on July 12 and 16, 2010 he unlawfully published defamatory matter on the Uganda Record when he published that government was behind the July 11, 2010 twin bombs that killed at least 76 Ugandans in the capital Kampala. Section 179 of Uganda's Penal Code Act states: "Any person who, by print, writing, painting, effigy or by any means otherwise than solely by gestures, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, commits the misdemeanour termed libel". The journalist's lawyer argues that it is improper to charge him under this law since it does not take into consideration online publications. The journalist was initially charged under sedition law, but the constitutional court subsequently declared this law unconstitutional on the back of an appeal by journalists, and so defamation charges were then preferred against the journalist.[29]

Security agencies also confiscated the journalist's laptop and mobile phone. Shortly after his arrest, the site http://www.ugandarecord.co.ug went down and has not been active ever since. It was not clear whether this resulted from pressure on the hosts or it was a decision taken by the publisher. The case against the online publisher was on-going in courts of law as of July 2012.

One analyst stated that the most significant aspect of the charging of the *Uganda Record* journalist was that the government was becoming interested in what Ugandans were writing online and was doing something about it. "The passing, in the immediate aftermath of the 7/11 [July 2011] bombings, of The Regulation of Interception of Communications Bill, will likely embolden the government to go after online work more aggressively. It will snoop around more, hacking into people's emails in the name of ensuring national security," he stated.[30]

**Newspaper website blocked at election time:** in February 2006, the government blocked access to private station 93.3 KFM and the website of its sister newspaper Daily Monitor (www.monitor.co.ug) because they were publishing independently tallied results. The paper's Managing Director said the internal affairs minister had explained to him the cause of the blockage but promised to end within two days.[31] The website became accessible before the two days period, by which time the elections commission had announced results from almost all over the country.

**Access to online publisher blocked:** In February 2006, UCC reportedly instructed ISPs to block access to www.RadioKatwe.com, a website that published anti-government gossip. Authorities alleged that the website was publishing "malicious and false information against the ruling party – National Resistance Movement and its presidential candidate." It was reported at the time that

[28] Uganda Opposition Calls for MTN Boycott, March 2011. http://telecomafrica.blogspot.com/2011/03/ugandas-opposition-calls-for-mtn.html

[29] ACME, Court Adjourns Online Journalist's Case, 18 January 2012, http://www.acme-ug.org/news/item/199-court-adjourns-online-journalist%E2%80%99s-case

[30] ACME, Be afraid, the government is nosing around online, Thursday, 12 May 2011, http://www.acme-ug.org/component/k2/item/26-be-afraid-the-government-is-nosing-around-online

[31] The Monitor, Govt Jams Monitor Radio, Site, February 26, 2006

MTN had issued a statement quoted by The Monitor, defending the decision to block the site, saying that Ugandan law "empowers the commission to direct any telecoms operator to operate networks in such a manner that is appropriate to national and public interest." [32] Access to the website was later restored. However, the website's administrators have since shut it down.

[32] CPJ, Critical website Radio Katwe blocked on eve of presidential election, 23 February 2006; http://www.ifex.org/uganda/2006/02/23/critical_website_radio_katwe_blocked/

## Conclusions

Uganda's Electronic Transactions Act is a positive development for the limitation of intermediary liability. Such legislation does not exist in many countries on the continent and beyond. However, still in its infancy, it remains to be seen whether such protections will be enforced and obeyed. Indeed, various other national legislations provide sufficient grounds for authorities to take actions against internet intermediaries. While authorities that may play a role are specified in some detail – for instance including the communications regulators, the defence and internal affairs ministers, courts and security officers – the procedures and the specific instances in which sanctions may be imposed are not very clear. Even with the increased internet usage and a vibrant telecommunications sector, penetration and accessibility for the majority of Ugandans remains relatively low. As such, legislations and regulations regarding the actions and subsequent liability of internet intermediaries are relatively new, and most of the legislation is not specific or exhaustive. Indeed, the government of Uganda is yet to clearly outline and implement a due process in terms of notice and take down procedures, time frames and roles of intermediaries in content moderation, removal and blocking. It appears that in the few cases involving obligations of intermediaries to control content over recent years, authorities evoke sections of the law only in instances of perceived anti-regime or pro-opposition activity. Such scenarios also appear to infringe on freedom of expression.

## Recommendations

- There is a need for advocacy around the role of intermediaries in keeping the content on the Internet free. Governments should adopt clear guidelines concerning what content is deemed as liable for removal and the steps that need to be taken to remove or block such content. Where takedowns have been directed or implemented, an appeals process which represents the interests of all relevant stakeholders including content creators, and provides measures for re-instating content that has been illegitimately removed is necessary.
- There is a need to create a strong service providers' association like UISPA and strengthen consumer groups by expanding their memberships to include other intermediaries. These should be enabled to advocate for progressive legislations related to intermediate liability.
- There is a need for coalitions involving civil society, media and the private sector to create awareness nationwide on how intermediate liability could be abused to harm individuals' freedoms online.
- There is a need for stronger advocacy campaigns for policies that protect intermediaries as platforms for freedom of expression and speech.
- Internet intermediaries should provide clear, accessible and understandable privacy options, backed-up by privacy-friendly default settings, minimising and anonymising the collection of personal information; hence assisting users in controlling their personal data. This will shape how internet users perceive and manage their personal information hence positioning intermediaries to provide mechanisms and assurance to protect user rights including privacy.