

State of Digital Rights in Uganda 2019

Surveillance and Democracy:
Uganda's Chilling Tales

State of Digital Rights in Uganda 2019

Surveillance and Democracy:
Uganda's Chilling Tales

□ About this Report

UnwantedWitness has been following the evolution and development of the digital landscape in Uganda, monitoring and documenting digital rights trends in relation to procurement and the use of surveillance technologies, data protection and privacy, the clamp down on independent media and the application of cybercrime laws, among others.

As human rights transition to online, there exist numerous impediments to full enjoyment of digital rights by the majority of Ugandans.

The report therein provides a trends analysis of surveillance tools augmented by facial recognition and artificial intelligence that are playing an increasingly prominent role in facilitating government control over citizens.

This is exacerbated by location monitoring, phone-tapping and biometric use. Data and technology are a reflection of power and control by those who collect the data, threatening the enjoyment of fundamental freedoms including the right to privacy, freedom of expression and civic space.

Incredible amounts of personal data, including sensitive personal data, continue to be collected in a manner that disregards the standards set by the law.

In discussing this topic, Unwanted Witness provides engagement and guidance to ensure that the law upholds the international human rights obligations to protect the right to privacy and other fundamental rights.

Free media and civil society's operating space continue to experience extra-legal harassment and intimidation under state influence using the police and security agencies to arrest, interrogate and convict activists, journalists and opposition politicians. The report provides a case scrutiny and the application of the law.

The annual State of Digital Rights report is significant for both state and non-state actors to rethink the pervasive use of technology and ensure that the public has a voice in how technologies are used and impact on their lives and societies.

□ Table of Contents

| | |
|---|----|
| Abbreviations and Acronyms | 4 |
| 1.0 Introduction and Background | 5 |
| 2.0 Surveillance, Cyber security and Elections | 7 |
| 2.2 The Right to Privacy | 13 |
| 2.2.1 National Identification Cards and Databases | 14 |
| 3.0 Censorship, Social Media snooping and Arbitrary Arrests | 16 |
| 3.1 Arbitrary Arrests, Interrogations and Detentions | 16 |
| 4.0 Online Content Restriction and Blocked Websites | 22 |
| 5.0 Social Media Tax (OTT) Shrinks the Digital Space | 25 |
| 5.1 Social Media routed through VPNs | 26 |
| Recommendations: | 26 |

Abbreviations and Acronyms

| | |
|------|--|
| CCTV | Closed Circuit Television |
| CID | Criminal Investigation Department |
| NIRA | National Identification Authority |
| NITA | National Information Technology Authority |
| NIN | National Identification Number |
| OTT | Over-the-Top tax |
| RICA | Regulation of Interception of Communications Act |
| SIM | Subscriber Identification Module |
| UCC | Uganda Communications Commission |
| UN | United Nations |
| UPF | Uganda Police Force |
| UW | Unwanted Witness |
| VPN | Virtual Private Network |

□ 1.0 Introduction and Background

As people transition to the online world, so do human rights. In Uganda, President Yoweri Museveni and his government have led the country for over 30 years and with the desire to maintain their grasp on power, they are beginning to see the Internet more as a political risk than human right or an economic opportunity.

The Internet is a driver of transformation providing alternative tools to facilitate service delivery, expression, electoral and democratic processes. Social media platforms like Twitter, Facebook, WhatsApp, Skype etc., have provided relative safety to build civic activism and competency to influence the political, social and economic agenda in Uganda.

Uganda's Internet penetration and Internet subscriptions in 2019 stood at 37.9% of the population and 15.2 million respectively aggregating to a total number of 23 million Internet users, a growth attributed to the 0.8% increase in demand for smartphones.¹

Internet usage has equally attracted draconian cybercrime laws with provisions giving those in positions of political power the opportunity to muzzle online activists, journalists, bloggers and netizens.

Cyber laws in Uganda like the Computer Misuse Act 2011, Regulation of Interception of Communications Act 2010 (RICA), and other related laws are manipulated by the state apparatus to suppress citizens' digital rights perpetrated by government departments, authorities and agencies to thrust regime critics from the online space because of the unease their influence creates across national and international forums about the regime.

In 2019, the country's defense budget hit a 3.5 trillion shillings² mark making it the second-largest portion of the national budget with clauses of "classified expenditure" to invade public scrutiny, signifying the state's commitment to boost high-level surveillance technology under the guise of national security.

The CCTV surveillance systems are supplied by Huawei, a Chinese company that helps to train personnel within security agencies on their use. Countries purchasing this technology have an inclination to be like-minded with China with a mission to maintaining the status quo of

1 <https://pctechmag.com/2020/02/uganda-internet-penetration-stands-at-37-9-with-23m-users/>

2 <https://www.parliament.go.ug/news/3271/defence-seeks-shs35-trillion-budget-proposal>

authoritarian leaders. China has in the recent past proved to be a technological advancement partner for Africa.

The desire by Museveni's regime to have Chinese-funded development at the expense of human rights and democracy is a ploy by China to expand its foreign policy.

Dependency on Chinese-shared global digital infrastructures raises the chance of intrusion in people's cultures and privacy.

In case of a privacy breach, there is a risk of failure by the Ugandan state to prosecute and extradite perpetrators across international borders since foreign satellite system operations are not located in the orbital space of Uganda.

This 2019 report provides a trends analysis and an overview of actions by both state and non-state actors in Uganda that pose risks to digital rights entrenched under most international laws and standards. Discussions in the report will centre around smart policing, surveillance, online censorship, arrests and detention, the OTT, criminalising dissent and online journalism, and the ramification for democracy and human rights in Uganda.

□ 2.0 Surveillance Cyber security and Elections

During the year under review, the government of Uganda continued undertaking communication and open space surveillance, social media snooping and data mining, among others.

While human rights law provides definite restrictions on the use of surveillance tools, including oversight and authorisation, the government of Uganda conducts unlawful surveillance in total disregard of human rights law and norms.

Communication surveillance in Uganda is primarily regulated by the Regulation of Communications Act, 2010 (RICA), particularly section 3 which provides for the establishment of a “Monitoring Centre” while section 8 mandates all telecommunications service providers to install relevant equipment with the capability of intercepting communications and also ensure that subscribers register their phone and data SIM Cards.³

The law has been criticised by Amnesty International for lack of adequate safeguards to ensure respect and protection of human rights, in particular the right to freedom of expression and the right to privacy.⁴

There is no clear oversight mechanism to RICA, making it easier for law enforcement authorities to track and monitor people and threatening the freedoms of vulnerable groups.

Later, the government through the national telecommunications regulator, the Uganda Communications Commission (UCC), introduced mandatory SIM card registration in 2012, using multiple Identification documents.

However, the requirements were later revised in March 2019, calling for verification and validation of all SIM cards, limiting the exercise to only a national identity card for nationals and passport for foreigners, including biometrics.⁵ These new requirements for SIM card registration are not only legally void but fall short of international human rights norms and standards, facilitating mass communication surveillance.⁶

3 <https://www.unwantedwitness.org/cyberpolicy/wp-content/uploads/2018/02/Regulation-of-Interception-of-Communication-Act-2010-1.pdf>

4 <https://www.amnesty.org/fr/documents/AFR59/016/2010/fr/>

5 <https://allafrica.com/stories/201903290158.html>

6 <https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/>



SIM card registration undermines people's ability to communicate anonymously, organise and associate. In addition, Ugandans who lack national IDs are excluded from accessing SIM cards, hence eliminated from participating in important spaces for formulating and sharing ideas.⁷

Surveillance tools augmented by facial recognition and artificial intelligence have played an increasingly prominent role in facilitating government control over citizens and blunting political challenges from opponents.⁸

Previous UN mandate holder emphasized that states must take measures to prevent the commercialisation of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies, considering their ability to facilitate systematic human rights violations⁹ This call remains relevant to Uganda today.

Towards the end of the 2017/2018 financial year, the parliament of Uganda passed a supplementary budget of 60 billion shillings (over \$200 million) for the second phase of the procurement of CCTV Cameras, under a contract awarded to Huawei.¹⁰

China's proliferation of digital authoritarian tools presents serious challenges from a country that lacks public scrutiny and oversight mechanisms, as the technology is likely to be used to quell mass protests and monitor opposition politicians.

7 <https://www.theeastafrican.co.ke/business/Uganda-SIM-card-registration-woes/2560-5144088-lq2lqh/index.html>

8 <https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9>

9 A/HRC/23/40, para. 97

10 <https://www.unwantedwitness.org/chinese-firm-supplies-900-surveillance-cameras-to-uganda/>



Some of the CCTV cameras along roads in Kampala.

In August 2019, an investigative report by the Wall Street Journal revealed how Huawei technicians had assisted Uganda police personnel to break into encrypted communication for opposition member of parliament Robert Kyagulanyi, also known as Bobi Wine.¹¹ The police and Huawei denied the report.

However, it is difficult for individuals or groups targeted by unlawful or arbitrary surveillance to bring claims against government agencies, partly due to structural barriers. Both legislature and the courts may bar these claims when they grant excessive defense to perceived national security and law enforcement interests.

In November 2019, President Museveni commissioned the National CCTV Command Monitoring Centre, at the police Headquarters in Naguru, Kampala.¹²

The Monitoring Centre collects data from 2,547 CCTV Cameras covering 1,038 locations within the Kampala Metropolitan Police area.¹³

More pervasively, the Uganda Police Force (UPF) is planning to integrate data from CCTV Cameras and forensic system with other key personal data collecting agencies like National Identification Registration Authority (NIRA), the national tax agency, the Uganda Revenue

11 <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>

12 <https://twitter.com/KagutaMuseveni/status/1200120752114196481>

13 <https://theinsider.ug/index.php/2019/07/02/uganda-police-full-statement-on-cctv-cameras-progress/>



President Museveni inspecting the CCTV Command monitoring center at police headquarters, Naguru (photo by PPU)

Authority, and the immigration department.¹⁴

“We intend to link the social cameras to police network which will improve on crime prevention and investigation process. We also plan to integrate the system with other stakeholders such as NIRA, Immigration, URA, NITA, the criminal justice system, among others, for purposes of sharing information,” the Inspector General of Police, Okoth Ochola, told President Museveni during the commissioning of the monitoring centre.

This however raises concerns over cyber security and the increased surveillance of dissents, human rights defenders and journalists. Privacy is not just important for journalists, but crucial for free expression in a wide range of civic situations and actions.

As reported by the Wall Street Journal, China has built half of the world’s current 1,000 smart city projects. China’s commitment to smart cities was firmly established by the Chinese government in its 12th Five-Year plan announced in 2011.¹⁵

14 <https://www.softpower.ug/police-to-integrate-its-cctv-forensic-systems-with-ura-nira-immigration/>

15 <https://www.usnews.com/news/cities/articles/2020-01-31/are-chinas-smart-cities-really-surveillance-cities>

The CCTV system in Uganda is part of Huawei's Safe City Initiative rolled out over 200 cities around the world, a company that has been put in the spotlight over allegations and fears of spying on citizens using facial recognition technology on behalf of the governments where their equipment is supplied.



Under China's Safe City Initiative, Huawei also provides technical assistance to officers of the Uganda Police Force. In November 2019, the Huawei team conducted a skills training for the senior Uganda Police force on "critical incident management."

Surveillance in Uganda flouts the state's international human rights obligations which mandate the government to put in place a legal framework that is publicly accessible, clear, precise, comprehensive and non-discriminatory and that any interference with the right to privacy must not be arbitrary or unlawful.¹⁶

16 U.N. Doc. A/RES/69/166

Next year, 2021, Uganda will be conducting general elections, with the incumbent President Museveni already endorsed by his ruling National Resistance Movement party to contest for the fifth term as a sole candidate.¹⁷

The endorsement followed a 2017 chaotic constitutional amendment of Article 102(b) of the 1995 Uganda Constitution, scrapping the upper age limit of 75 years as eligibility for the presidency.¹⁸ This was a move to establish a life presidency for Museveni, pushing Uganda's democracy off a cliff.

Evidence shows that human rights violations are always high during Uganda's election period. During the recent elections in 2016, the government blocked all social media platforms under the pretext of maintaining public order. More concerning is the lack of publicly known oversight and accountability mechanism for the sprouting of this surveillance in Uganda.

Social Media snooping and restrictions violate a right to privacy, enabling discrimination and restricting freedom of expression/association.

Individuals are less likely to join certain groups of interest for fear of having their activities monitored. Such actions drive citizens into self-censorship, downplaying their democratic participation.

As Uganda is heading for the 2021 elections, it is critical to monitor the social media platforms to ensure that they do not become sources of disinformation with false, shocking, negative, exaggerated and emotionally charged content in favor of particular candidates.

There is also need to regulate the use of social media surveillance tools by government agencies and law enforcement and prevent their use to favor their agenda.

Today with the growing use of smart policing technologies that are short of transparency and legal mechanisms, concerns over using surveillance technology to violate democratic process need to be heeded.

Importantly, the incompatibility of mass surveillance with human rights requires urgent attention in order to safeguard democracy and protect journalists, activists, human rights defenders and government critics from intrusion into their privacy.

17 https://www.youtube.com/watch?reload=9&v=WSUAE6vs_ig

18 <https://www.xinhuanet.com>

2.2 The Right to Privacy

Privacy is a fundamental right enshrined in the 1995 Uganda constitution as well as in international human rights law. The right to privacy is increasingly relevant to Ugandans, as is the protection of individuals' data.

Article 27 of the 1995 Uganda Constitution¹⁹ guarantees the right to privacy, further recognised by Article 17 of the International Covenant on Political and Civil Rights (ICCPR).

Uganda became the first East Africa country to recognise privacy as a fundamental human right, by enacting a data protection law.

The Data Protection and Privacy Act, 2019, which was passed on February 25, 2019, aims to protect individuals and their personal data by regulating processing of personal information by state and non-state actors, both within and outside Uganda.²⁰

Protecting personal data in the digital age is essential to effective democratic governance. However, despite having a data protection legislation in place for over one year now, Uganda lacks the institutional framework, processes and infrastructure to support law enforcement and meaningful protection of data privacy rights.

According to a blog post authored by Unwanted Witness Uganda to mark the law's 1st anniversary, the lack of enforcement mechanism has rendered the law toothless.²¹

It was noted that state and non-state actors have never taken any measures to change their policies and practices as per the obligations under the data protection Act, as incredible amounts of personal data, including sensitive personal data continues to be collected in a manner that disregards the standards set by the law.

Government has intensified mandatory collection of sensitive personal data as seen with the national identification system, smart policing through the use of CCTV cameras and the use of a virtual court system, among others.

19 https://www.unwantedwitness.org/cyberpolicy/wp-content/uploads/2018/02/Constitution_of_Uganda-1.pdf

20 <https://www.unwantedwitness.org/download/uploads/THE-DATA-PROTECTION-AND-PRIVACY-ACT-2019-min.pdf>

21 <https://www.unwantedwitness.org/one-year-on-what-has-ugandas-data-protection-law-changed/>

2.2.1 National Identification Cards and Databases

The Parliament of Uganda passed the Registration of Persons Act, 2015 to harmonise existing laws on the registration of persons, establishing a single central registration body and a national identification register of all persons in Uganda.²²

The act established the National Identification and Registration Authority (NIRA), overseeing the issuance of national identity cards. The law makes it mandatory for all Ugandan citizens of 16 years and above to register with the Authority and acquire national identity cards, register for death and birth and issue certificates.

Establishing every person's legal identity including birth registration by the year 2030 is the aim of Sustainable Development Goal (SDG) 16.9

Issuance and self-assertion of IDs is key to empowering citizens to engage in the modern economy, but also comes with significant risks.

According to media reports, by early 2019 over 17 million Ugandans had obtained IDs and allocated a unique National Identification Number (NIN) while 2.4 million still lacked IDs.²³

However, this figure keeps changing as many Ugandans either lose their national IDs or turn 16 years old, the eligibility age for national ID.

In May 2019, an investigative report published in a government newspaper, the Sunday Vision, revealed a racket of corruption within the ID system indicating that foreigners were acquiring IDs at 100,000 Uganda shillings (\$27.8), which was later refuted by the registration agency, NIRA.²⁴

Similarly, a preliminary report published by Unwanted Witness titled 'Uganda's Digital ID System: A Cocktail of Discrimination,' revealed further disturbing and significant risks to the enjoyment of human rights, ranging from data privacy to inequality and exclusion.²⁵

22 <https://ulii.org/ug/legislation/act/2015/4-6>

23 <https://www.monitor.co.ug/News/National/2-4-million-Ugandans-don-t-have-national-IDs/688334-4970294-ohwoha/index.html>

24 <https://www.nira.go.ug/wp-content/uploads/Publish/PRESS%20STATEMENT2.pdf>

25 <https://www.unwantedwitness.org/download/uploads/UgandaE28099s-Digital-ID-System.pdf>



Despite the controversy surrounding the design and implementation of Uganda's ID system, access to essential services are dependent on a national ID for all citizens. The drive for identification has thus become a generator of data about Ugandans, linking together different aspects of their lives under a single identity.²⁶

In his latest report, the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, noted that the emergence of the digital driven welfare states in many countries across the globe is increasingly driven by digital data technologies that are used to automate, predict, identify, surveil, detect, target and punish.²⁷

In the neighboring Kenya, the High Court issued an interim order allowing the registration process to continue but on a voluntary basis. The disbursement of government services and benefits could not be made conditional on participation, the court ruled. The court order followed a petition by a human rights advocates group claiming that the Huduma Namba programme violated the right to privacy, equality, non-discrimination and public participation.²⁸

26 <https://www.unwantedwitness.org/ugandas-id-system-breeding-automated-exclusion/>

27 <https://www.hrw.org/news/2019/05/21/submission-un-special-rapporteur-extreme-poverty-human-rights-regarding-his-thematic>

28 <https://www.standardmedia.co.ke/article/2001334286/you-ll-miss-vital-services-without-huduma-namba>.

□ 3.0 Censorship, Social Media snooping and Arbitrary Arrests.

Uganda's civil society and media sector have remained vibrant despite suffering extra-legal harassment and intimidation under the state using the police and security agencies to arrest, interrogate and convict activists, journalists and opposition politicians. The government agencies violate human rights with impunity through pressure from the First Family, influential public servants and pro-government politicians.²⁹

This is contrary to international human rights law, particularly Article 9 of the Universal Declaration of Human Rights which stipulates that “no one shall be subjected to arbitrary arrest, detention or exile”; that is, no individual, regardless of circumstances, is to be deprived of their liberty or exiled from their country without having first committed an actual criminal offense against a legal statute and the government cannot deprive an individual of their liberty without due process of law.

3.1 Arbitrary Arrests, Interrogations and Detentions

In many cases, individuals arrested over cybercrimes are given no explanation as to why they are being arrested or detained. The officers-in-charge of these operations produce no arrest warrants or detention orders to the suspects, leaving room for manipulation of the law.

Those arrested and detained are usually held incommunicado for the first few days and their whereabouts sometimes concealed only to be bailed out through Habeas Corpus applications to the courts of law by legal representatives and pressures from families, friends and the public expressed through peaceful demonstrations, online campaigns or hashtags.

Throughout the year, Unwanted Witness has documented cases in which at least 13 Ugandans were either arrested, summoned or interrogated at Police's Criminal Investigations Department (CID) for their online engagements.

The majority were charged under the Computer Misuse Act, 2011 on charges of offensive communication and cyber harassment.

29 <https://www.monitor.co.ug/News/National/Arrested-Musevenis-name--Kabuleta-Enanga-Moses-Nsubuga/688334-5194994-4ua0xr/index.html>

It is also common practice for suspects to be held for periods longer than the constituted 48 hours, a violation of article 23(4) (b) of the 1995 Uganda constitution.³⁰ During the arrests, interrogations and illegal detentions, the suspects suffer physical and psychological torture.

On July 13, 2019, an evangelical pastor and journalist Joseph Kabuleta was arrested and detained at the army's Special Investigations Unit in Kireka on the outskirts of Kampala for four days without trial³¹ over his Facebook post under his Weekly Rant where Kabuleta referred to President Museveni as "a gambler, thief and liar".³²

With neither a warrant of arrest nor police summons, Kabuleta was blindfolded from Lugogo in Kampala and driven to the Special Investigation Unit in Kireka by plain clothed security operatives. He was interrogated, drenched with water and stripped naked amidst physical torture causing a nose bleed. He was released on Police bond following family and public pressure and cautioned to disassociate with the media.³³

Ison Rocky, a website developer and platform manager at Watchdog Uganda,³⁴ was on June 18, 2019 picked from his workplace by plain clothed men disguising as potential clients. The men were later identified as police investigative officers attached to the Electronic Crime Counter Measures Unit at CID headquarters, Kibuli in Kampala where Ison was taken for interrogation and detention.

Police then extended the crackdown to two other Watchdog journalists, Mike Ssegawa and Moses Bbule.³⁵

30 <https://uls.or.ug>

31 <https://www.monitor.co.ug/News/National/Police-release-Kabuleta-four-days-after-his-arrest/688334-5198866-xs240y/index.html>

32 <https://www.monitor.co.ug/News/National/688334-5194070-or7sptz/index.html>

33 <http://www.pmldaily.com/news/2019/07/kabuleta-released.html>

34 www.watchdoguganda.com

35 <https://www.unwantedwitness.org/news-brief-uganda-police-detains-and-charges-a-website-developer-with-defamation/>



Watchdog publishers, digital activist and lawyers at CID headquarter, Kibuli (photo by Emma Magambo)

The trio were charged under the country's cybercrime legislation, Computer Misuse Act, 2011, which is being enforced by the Electronic Crime Counter Measures Unit. In 2018, Unwanted Witness scrutinised the mandate and activities of this little-known unit and observed that it is not clear to which legal and regulatory obligations the unit is subjected.³⁶

The lack of transparency in the mandate and activities of similar organs shields them from public scrutiny, thus breeding human rights abuse.

The Leadership Code of conduct requires public servants to declare their wealth to be known to the public but this was put to a test in February 2019 when police summoned five editors - Richard Wanambwa (Eagle online), John Njoroge (CEO magazine), Dennis Irumba (Spy Uganda), Raymond Wamala and Bob Atwine to the CID to record statements on criminal libel and offensive communication charges on allegations of publishing photographs of buildings and bank accounts allegedly belonging to the Bank of Uganda deputy governor Louis Kasekende.

36 <https://www.unwantedwitness.org/>

The 1995 Uganda Constitution Article 41(1) clearly states that every Ugandan citizen has a right to access information in possession of the state or agency although the law restricts interference with a person's privacy.

But by virtue of the deputy governor's public office, investigation into the accumulation of his wealth has to be brought under public scrutiny. The summons was, therefore, uncalled for.

The same cybercrime law (Computer Misuse Act) 2011 was used to arrest Dr. Stella Nyanzi in November 2018 for the criticising President Museveni and on the 21st day of June, 2019, a magistrate Gladys Kamasanyu ruled that Dr. Nyanzi had a case to answer in relation to offenses of cyber harassment and offensive communication contrary to Section 25 of the Computer Misuse Act 2011.³⁷



Extreme Left: Dr. Stella Nyanzi in the dock at Buganda Road court.

After a contested due process³⁸ in early August 2019, Nyanzi was charged and sentenced to 18 months in Luzira Prison for harassing President Museveni who never appeared in court as a witness.³⁹ The decision was criticised by human rights activists who accused the government of using cybercrime laws to stifle political dissent, freedom of speech and expression.

37 <https://www.aljazeera.com/news/2019/08/ugandan-academic-stella-nyanzi-jailed-harassing-museveni-190803141817222.html>

38 <https://twitter.com/RosebellK/status/1231561176473051136>

39 *ibid*

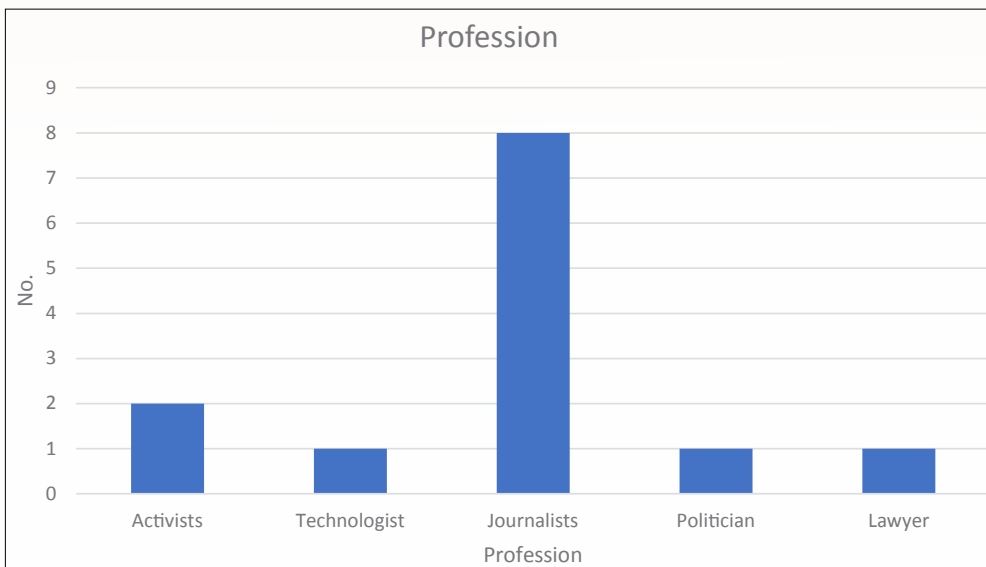
In this 2019 report, most of the cyber cases are based on allegations of misuse of the computer under which charges of offensive communication and cyber harassment fall. Online pictures, songs, poems, artistic impressions or opinions criticising the president and the regime sympathisers always leave the authors vulnerable to ruthless state action.

Unwanted Witness along with two others in 2017 petitioned the Constitutional Court, challenging the constitutionality of section 25 of the Computer Misuse Act 2011.⁴⁰ The charge of offensive communication has been extensively and repeatedly been used to gag freedom of expression and opinion on the Internet.

The wording under sections 24 and 25 like ‘obscene’, ‘lewd’, ‘indecent’, ‘lascivious’, ‘quiet’, ‘disturb the peace’ are not defined clearly, leaving this open to subjective judicial interpretation by the officer in charge of the matter, contrary to article 28(12) of the 1995 constitution which states that: “Except for the contempt of court, no person shall be convicted of a criminal offence unless the offence is defined and the penalty for it is prescribed by law.”⁴¹

These sections give the Director of Public Prosecution (DPP) prosecutorial powers over alleged offenders which has resulted in selective prosecutions of Internet users based on certain views deemed objectionable by the government. These powers need to be trimmed and checked to harmonise human rights practice with the international legal framework.

A bar graph showing the number of those arrested, summoned and detained, by profession

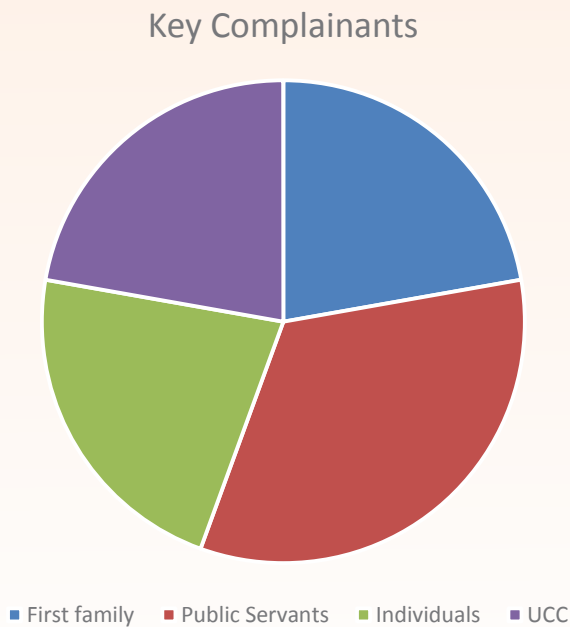


40 <https://www.unwantedwitness.org/?s=consitutional+petition#>

41 <https://www.facebook.com/Barefootlaw/posts/under-article-28-of-the-constitution-no-person-shall-be-convicted-of-a-criminal-/432344630177446/>

Online journalists were persecuted most, followed by activists and politicians. Any criticism of the First Family and the ruling government resulted in those who expressed their discontent summoned, arrested, detained or their online content restricted.

A pie chart showing key complainants



In 2019, the key complaints were mainly from public servants followed by the First Family, individuals and the Uganda Communications Commission. Topics in media about the military, president’s family, the oil sector, land grabbing and public servants are considered taboo in Uganda’s online space.

□ 4.0 Online Content Restriction and Blocked Websites

The government penalised those who published items contrary to its guidelines, through direct or indirect censorship and threatening to withdraw licensing and advertising rights, a political action that was managed and executed by the Uganda Communications Commission through the issuance of suspensions and notices.



On August 5, 2019, the UCC introduced a US\$20 (about 73,800 Uganda shillings) fee to be paid by social media influencers and publishers to obtain a license. It was a tactic intended to remind online publishers of the law and regulations as they publish their content online, as stated by the UCC spokesman Ibrahim Bbosa. This action blurred the boundary between cyberspace and territorial Uganda.

Unwanted Witness in 2018 petitioned the Constitutional Court over a similar violation challenging the UCC directive requiring all online publishers to acquire licenses.⁴² UW, objecting to Section 2 of the Uganda Communication Commission Act 2013, disagrees with the definition of “communication services” as being overly vague and broadly inconsistent with Article 29(1) and 27(2) of the 1995 Ugandan constitution.

42 <https://www.unwantedwitness.org/unwanted-witness-petitions-court-over-online-licenses/>

In February 2019, UCC ordered the Daily Monitor newspaper to cease publication of content on its website, pending clearance from the Commission. The Daily Monitor was accused of being non-compliant with a directive issued in March and April 2018 that required online newspapers to register.⁴³

The directive, however, came after a complaint by the Speaker of Parliament, Rebecca Kadaga, to the UCC director Godfrey Mutabazi about an online article published by the Daily Monitor that associated her with the practice of witchcraft, something she feared would damage her reputation.⁴⁴

The human rights lawyer Eron Kiiza, who in 2019 was handling a case involving residents of villages in Mubende district who were evicted from their land by powerful persons linked to the state, frequently wrote posts on Facebook citing bias in how the case was being handled by the Resident High Court judge Joseph Murangira of Mubende.⁴⁵

The Uganda Law Society President Simon Peter Kinobe on July 18 ordered Kiiza to take down the Facebook posts, arguing that comments in the media by an advocate in personal conduct are contrary to the advocate's "professional" conduct and in this particular case bordered on criminality. A conflict of interest was manifested in this paradigm.

On July 11 2019, Harrison Simiyu, a senior nursing officer attached to Kwirwot Health Centre II in Bukwo district, was interdicted from office over misuse of social media in a letter signed by the Chief Administrative Officer (CAO) Mr. Gabriel Atama. In his defense, Mr. Harrison Simiyu explained that this was after her exposed corrupt district officers using a social media platform.⁴⁶

43 <https://www.monitor.co.ug/News/National/Oryem-Nyekko-banned-UCC-Uganda-media-suppressing/688334->

44 <https://observer.ug/news/headlines/59840-ucc-suspends-daily-monitor-website-over-kadaga-witch-story>

45 <https://observer.ug/news/headlines/61389-uganda-law-society-asks-lawyer-to-pull-down-facebook-post>

46 <https://www.monitor.co.ug/News/National/Nursing-officer-interdicted-over-defaming-officials-social-media/688334-5190984-c5sck4z/index.html>

On August 22, 2019, the UCC ordered Internet Service Providers (ISPs) to block access to the website of the Rwandan daily, the New Times, saying the paper published harmful propaganda against Uganda and was a threat to national security.⁴⁷

A day later, Rwanda retaliated by blocking Uganda online news websites like the Observer, New Vision, Nile Post, Softpower, Daily Monitor and the Independent. The political tension between the two countries' heads of state stifled people's right to access information.

Government has an oversight role to regulate freedoms of association, press, assembly, speech and others but does not have the right to prevent them. The use of the UCC and the regime's operatives to restrict online content through baseless accusation of breaching the Minimum Broadcasting Standards and operating guidelines is illegitimate.

47 <https://www.pmldaily.com/business/tech/2019/08/ucc-moves-to-block-rwanda-websites-for-promoting-hate-speech.html>

□ 5.0 Social Media Tax (OTT) Shrinks the Digital Space

In 2019, the social media tax turned one year. President Museveni, the mastermind behind it, had hoped that imposing this tax would silence the voice of the majority against his rule and curtail freedom of speech. Although government officials looked at the tax as a source of revenue, it is already taking a toll on Internet users in the country, negatively affecting digital inclusion in the country.⁴⁸

Affordability and access to the Internet is still a challenge in Uganda. A daily charge of 200 Uganda shillings (\$0.05) as a tax to log on social media platforms increases the cost of Internet use.⁴⁹

UCC reported that the number of Internet users had dropped by 30% in January 2019, also noting a downward trend in the use of ICT among the people with disabilities.

The statistics above match the findings of the report by the parliamentary committee on ICT, which noted that the social media tax had negatively impacted on the consumption of ICT services and products. The government overestimated the gains from the new tax which saw only a 17% increase in revenue.⁵⁰

The #ThisTaxMustGo campaign against the OTT put the government under the spotlight and while the tax remains, it has a negative economic multiplier effect on ICT services and access in the economy.

Uganda falls short of the ICT4D goals since the ICT infrastructure cannot be expanded to the rural sector because of such taxes. Information technology platforms form the backbone for markets, inputs sourcing, service delivery and advisory services, leading to savings and increased productivity.

48 <https://techpoint.africa/2019/02/20/uganda-social-media-tax/>

49 <https://www.genderit.org/resources/offline-and-out-pocket-impact-social-media-tax-uganda>

50 <https://ugandaradionetwork.net/story/social-media-tax-payers-fall-to-6-8-million-internet-users>

5.1 Social Media routed through VPNs

In Uganda, VPNs have become a vital tool for those looking to keep their Internet browsing private, access blocked websites, and bypass the new over-the-top social media tax.⁵¹

Even though Ugandan citizens have been affected thus far, the use of VPNs has given relatively secure access and freedom on the Internet.

A survey by Whitehead Communications in 2019 found out that 57% percent of citizens were using VPN apps to evade the OTT. Ugandans mainly in urban areas are adopting VPNs to stay connected and engaged on social media platforms to share views and opinions.

The Internet should be maintained as an open platform on which network providers treat all content, applications and services equally. The future of Internet freedoms in Uganda rests on our ability to fix social media as a “free” space because social media platforms form the main entry point to online spaces in Uganda.


Recommendations:


- Government of Uganda should immediately halt procurement and use of intrusive surveillance tools until there is convincing evidence that the use of these technologies can be restricted to lawful purposes that are consistent with human rights standards of legality, necessity and legitimacy.
- Parliament should ensure that any legislation governing surveillance in Uganda is laid out in precise and publicly accessible laws and is only be applied where necessary and proportionate to achieve one of the legitimate objectives enumerated in Article 19(3) of the International Covenant on Civil and Political Rights.
- The Ministry of Information, Communication Technology should expedite commencement of an open, transparent and inclusive process of soliciting for citizens’ participation in the formulation of regulations and guidelines for the effective implementation of the Data Protection and Privacy law, in order to safeguard privacy and freedoms.
- Meaningful and conclusive investigations should be conducted before any cyber prosecution is considered by police, to avoid undue application of cybercrime laws to silence legitimate dissent.

51 <https://www.dw.com/en/uganda-one-year-of-social-media-tax/a-49672632>

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

 [Unwantedwitness-Uganda](#)

 [@unwantedwitness](#)

 [unwantedwitness](#)