

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	381
Land:	Uganda
Kilde:	Freedom House
Titel:	Freedom on the Net 2019 – Uganda
Udgivet:	4. november 2019
Optaget på baggrundsmaterialet:	21. maj 2021



Uganda

PARTLY FREE

56
/100

A. <u>Obstacles to Access</u>	14 /25
B. <u>Limits on Content</u>	23 /35
C. <u>Violations of User Rights</u>	19 /40

LAST YEAR'S SCORE & STATUS

59 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free)



Overview

Internet freedom in Uganda suffered as the government continued to crack down on online expression, including by blocking over two dozen

pornographic websites and imposing a tax on social media and communication platforms for the purpose of curbing “gossip. Reports about the government’s close collaboration with the Chinese technology firm Huawei raised concerns about surveillance as the 2021 presidential election approaches. During the reporting period, Huawei allegedly helped the government surveil prominent opposition Parliament member and presidential hopeful Robert Kyagulanyi, better known as Bobi Wine.

While Uganda holds regular elections, their credibility has deteriorated over time, and the country has been ruled by the same party and president since 1986. The ruling party, the National Resistance Movement (NRM), retains power through patronage, the manipulation of state resources, intimidation by security forces, and politicized prosecutions of opposition leaders.

Key Developments, June 1, 2018 – May 31, 2019

- In July 2018, the government implemented a controversial social media tax, requiring users on a number of popular social media platforms including Facebook, Twitter, and WhatsApp to pay a daily fee of \$0.05, which is prohibitively expensive for many users. Internet service providers (ISPs) were ordered to block over 50 social media and communications platforms for users until they paid the tax (see A2).
- In July 2018, the Uganda Communications Commission (UCC) directed ISPs to block a list of 27 websites for “streaming pornographic content” (see B1).
- In February 2019, the UCC instructed the *Daily Monitor* to suspend its website, ostensibly for failing to register the site as required by a 2018 government regulation. However, analysts contend that the order was made due to an unflattering story about the speaker of Parliament published on the website, which had elicited complaints from the speaker. The *Daily Monitor’s* website was never suspended, but the story about the speaker was removed (see B2).

- A 2018 report by Citizen Lab identified Uganda as one of the 45 countries worldwide using Pegasus, a targeted spyware software developed by Israeli technology firm NSO (see C5).
- A *Wall Street Journal* article published in August 2019 revealed close cooperation between the Ugandan government and Huawei, a Chinese technology company, to surveil opposition figures and government critics, including during the reporting period (see C5).

A. Obstacles to Access

A new social media tax instituted in July 2018 increased the cost of access for Ugandans and disproportionately affected poorer citizens. Significant gender and urban-rural divides persist in accessing the internet.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

2 / 6

Internet penetration rates have increased incrementally in recent years, up from 22 percent of the population in 2016 to an estimated 44 percent in 2017, according to the latest data from the International Telecommunication Union (ITU). ¹ However, the estimated number of internet users declined between 2017 and 2018, likely due to the introduction of a social media tax, known as the over-the-top (OTT) tax, in July 2018 (see A2). ² The most recent government data from the UCC, the communications regulatory body, estimated an internet penetration rate of approximately 35 internet users per 100 inhabitants in September 2018, ³ compared to 48.2 in September 2017. ⁴ The mobile phone penetration rate was to 57.3 percent in 2018, according to the ITU.

Internet speeds remain very slow, averaging 3.2 Mbps (compared to a global average of 11.3 Mbps), according to the 2019 report from Cable, a UK-based telecommunications company. ⁵ However, the National Broadband Policy adopted in September 2018 seeks to deliver a

minimum speed of 4 Mbps. ⁶ Other obstacles to internet access include limited access to electricity in rural areas.

New investments in Uganda's information and communications technology (ICT) infrastructure aim to improve connectivity, with some assistance coming from global technology companies. In April 2019, Nokia and Liquid Telecom announced upgrades to their fiber-optic network in East Africa, including Uganda. ⁷ In 2017, Facebook partnered with Airtel Uganda and Bandwidth & Cloud Service (BCS) to build a 770-kilometer fiber backhaul network in northwestern Uganda as part of its Telecom Infra Project. ⁸ Additionally, Google launched its first Wi-Fi network in Kampala as part of Project Link in 2015. ⁹

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

0 / 3

While internet access has become more affordable, particularly on mobile phones, costs are still expensive for many Ugandans. ¹ The introduction of a daily 200 Uganda shilling (\$0.05) tax on social media use in July 2018 (see B1) makes access effectively more expensive and may “push basic connectivity out of reach for millions,” according to the Alliance for Affordable Internet. ² The organization also reported that the new social media tax has disproportionately affected the poor, increasing the cost to connect for this group by 10 percent. ³ A September 2018 report from the UCC confirmed these fears by indicating a drop in the number of internet subscribers from 16 million to 13.5 million since its introduction in July 2018. ⁴ However, statistics from the Ministry of ICT reported 18.8 million internet users as of May 2019. ⁵

In order to enforce the tax, in July 2018, mobile telecommunications companies blocked access to 58 social media platforms, including Facebook, Twitter, and WhatsApp, ⁶ for all customers who had not yet paid. The imposition of the tax followed a directive from the president instructing the Finance Ministry to introduce taxes on OTT services with

the stated purpose of curbing “gossip” and improving the country’s tax base.⁷ In a Twitter poll conducted by the *Daily Monitor*, a majority of respondents (70 percent) reported that they bypass the tax by employing a virtual private network (VPN).⁸ In response, the executive director of the UCC instructed ISPs to either tax customers to use VPNs or block access to them.⁹ In July 2018, the Opera web browser became the first VPN platform to be blocked under the policy, by MTN Uganda.¹⁰ Also in July, the social media tax was challenged in court by a group of tech leaders who claimed it violated principles of net neutrality.¹¹

Uganda’s ICT and National Guidance Ministry, through the National Information Technology Authority–Uganda (NITA–U) has been developing the National Data Transmission Backbone Infrastructure project since 2007, which aims to ensure the availability of high-bandwidth data connections in all major towns at reasonable prices.¹² In 2016, the government began offering a free trial of wireless internet access in the Kampala Central Business District and parts of Entebbe.¹³

Only 24 percent of Ugandans live in urban areas¹⁴ and access to electricity is limited in rural areas, resulting in a significant urban-rural divide in internet access.¹⁵ There is also a notable gender gap in internet access: the Inclusive Internet Index notes a gap in connectivity of approximately 16 percent between men and women.¹⁶

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	6 / 6
---	--------------

There were no reports of politically motivated interference in mobile or internet networks by the government during the coverage period, aside from during the implementation of the OTT tax.

Section 5(1) (b) and (x) of the 2013 Uganda Communications Commission Act permits the communications regulator to “monitor, inspect, license, supervise, control, and regulate communications services” and to “set standards, monitor, and enforce compliance relating

to content.” ¹ The government has used this clause in the past to order ISPs to block mobile internet users’ access to OTT services such as WhatsApp and Facebook (see B1). Separately, the government ordered the shutdown of Facebook, Twitter, WhatsApp, and mobile money services for four days in the run-up to the 2016 elections and again ahead of President Museveni’s inauguration.

Uganda’s backbone connection to the international internet is privately owned in a competitive market. ² The country’s national fiber backbone is connected to the EASSy international submarine fiber-optic cable system that runs along the eastern and southern coasts of Africa. ³ Telecommunications providers are also connected to TEAMS (The East African Marine System) and SEACOM marine fiber-optic cables through Kenya. As of May 2019, 28 ISPs are connected to the Uganda Internet Exchange Point (UIXP). ⁴

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

5 / 6

There are no known obstacles or licensing restrictions placed by the government on entry into the ICT sector, and new players have entered the market with ease in recent years. However, the government is believed to exert some pressure on ISPs and the market structure.

The number of industry players has grown over the years, and many now offer comparable prices and technologies. Currently, there are 26 telecommunications service providers that offer both voice and data services, including MTN Uganda, Airtel Uganda, Uganda Telecom Limited (UTL), Africell Uganda (formerly Orange Uganda), Vodafone, Smart Telecom, and Afrimax, among others, ¹ which all offer 4G LTE network speeds. All service providers are privately owned except for UTL, which the government took full ownership of in 2017, following the withdrawal of 69 percent of the shares in the company by shareholders. ²

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

1 / 4

Uganda's telecommunications regulator, the UCC, has been criticized for its failure to operate in a free, fair, and independent manner. ¹ The body is mandated to independently coordinate, facilitate, and promote the sustainable growth and development of ICTs in the country. The UCC also provides information about the regulatory process and quality of service, and issues licenses for ICT infrastructure and service providers.

² The commission's funds derive mainly from operator license fees and a 2 percent annual levy on operator profits. ³

There is a general perception, however, that comprehensive and coherent information about the commission's operations is not always accessible, and that the body is not entirely independent from the executive branch of the government. ⁴ For example, the ICT minister has the authority to approve the UCC's budget and appoint members of its board with approval from the cabinet. There are no independent mechanisms in place to hold the UCC accountable to the public.

B. Limits on Content

In July 2018, the regulator issued a notice to all ISPs to block access to pornographic websites, while in March 2019, ISPs were instructed to block access to a gambling website. Additionally, in February 2019, the regulator ordered Monitor Publications, the publishers of the Daily Monitor, to immediately suspend its online newspaper services for publishing a story that was critical of the speaker of Parliament.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?

5 / 6

The government increased web censorship over the coverage period, in order to prevent access to pornography and betting sites, as well as to

enforce a tax on OTT services such as Facebook and WhatsApp (see A2).

In March 2019, the UCC issued a notice to ISPs to immediately block access to the gambling website BetPurse, citing concerns about illegal and unregulated online gambling operations. ¹

Pornography is illegal in Uganda and is a regular target for online censorship. In July 2018, the communications regulator directed ISPs to block a list of 27 websites for “streaming pornographic content;” the list was reportedly supplied by the Pornography Control Committee. ² The committee was established in 2017 and was reportedly allocated 2 billion Uganda shillings (\$535,000) to utilize new technologies that can monitor and intercept pornographic material. ³ The 2014 Anti-Pornography Law holds service providers criminally liable for the uploading or downloading of vaguely defined pornographic material on their systems, ⁴ with penalties of up to five years in prison and fines of 5 million Uganda shillings (\$1,300). ⁵

The government has a history of blocking access to social media and communications platforms altogether during politically sensitive moments. During the last general elections in 2016, Facebook, Twitter, WhatsApp, Instagram, and mobile money services were blocked for four days. ⁶ President Museveni declared the blocks a necessary measure to prevent people from using the platforms to “tell lies.” ⁷ Access to the platforms was restored three days after the elections, but was obstructed again the day before Museveni’s inauguration to another contested five-year term in office, for “security reasons.” ⁸

After the coverage period, in August 2019, the UCC ordered ISPs to block Rwanda’s *New Time* website in the midst of tensions between the two countries. ⁹ Several other Rwandan sites were reportedly blocked as well. ¹⁰

B2 0-4 pts

	2 / 4
--	--------------

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	
--	--

State and nonstate actors have employed legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete legitimate content.

In February 2019, the UCC instructed the *Daily Monitor* to suspend its website, ostensibly for failing to register the site as required by a 2018 government regulation. However, analysts contend that the order was made due to an unflattering story about the speaker of Parliament published on the website, which elicited complaints from the speaker (see B3 and B6). ¹ The website ultimately remained accessible, but the controversial story was taken down.

Online users have been forced to remove content from their social media pages, and the practice is likely underreported. In an anonymous interview in May 2018, a blogger claimed that he had been approached by security operatives and offered a bribe to remove content from his blog that was deemed “defamatory” to the government. ² Although he did not take the bribe or remove the content, he expressed fear for his life, which compelled him to cease writing about certain sensitive topics.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	2 / 4
---	---------------------

Restrictions on internet and digital content frequently lack proportionality to the stated aims. Service providers are governed under several frameworks that require them to filter, remove, and block content considered illegal by authorities. These include the 2013 UCC Act, ¹ the 2010 Regulation of Interception of Communication (RIC) Act, ² and the 2014 Anti-Pornography Act, ³ among others.

During the reporting period, the government ordered ISPs to block dozens of social media and communications platforms as a means of enforcing the new tax on OTT services (see A2). The tax and the means of enforcement are disproportionate to the stated goals of curbing gossip and increasing tax revenue. The UCC reported a significant reduction in internet users in the three months after the implementation of the tax (see A2). The figures confirmed fears that the tax would negatively impact internet access and affordability. ⁴

In 2017, Parliament passed the much-criticized 2016 Uganda Communications (Amendment) Bill, ⁵ which amended Section 93(1) of the 2013 Uganda Communications Act to eliminate the system of checks and balances on the ICT minister's supervision of the communications sector by removing requirements for parliamentary approval of regulations proposed by the ICT Ministry. ⁶ The ICT minister's increased power was on display when he ignored Parliament's motion to extend the deadline for SIM card reregistration, and instead directed the UCC to switch off all unverified cards in 2017. ⁷

After only 14 entities complied with new requirements instituted in March 2018 for news sites and blogs to register and obtain authorization from the UCC, the body issued a second directive in April ordering ISPs to block access to unregistered sites (see B6). ⁸ There were no updates on the number of websites registered or the number blocked for failing to register as of mid-2019.

In 2017, the digital rights and free expression groups Unwanted Witness Uganda and Article 19 sued the Ugandan government and service providers for the social media blocks during the 2016 election period, contending that the blocks violated citizens' fundamental rights. ⁹ The case was ongoing as of May 2019. ¹⁰

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?

2 / 4

The Ugandan government continued curtailing press and online freedoms during the coverage period, resulting in increased self-censorship among both online journalists and ordinary users.

Social media users are increasingly setting up pseudonymous accounts to protect their anonymity and avoid harassment. ¹ Taboo topics include the military, the president's family, the oil sector, land grabs, and presidential term limits. Nonetheless, blogging continues to be popular among young Ugandans and journalists who have boldly taken to the internet to report candidly on controversial issues such as good governance and corruption. ² According to 2016 research by the Africa Media Barometer, Ugandans “practice their freedom of expression, but not without fear.”

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

3 / 4

The online information landscape remains generally free from overt government manipulation or control. However, the government's continued focus on regulating social media content was observed during the reporting period, with the introduction of the OTT tax in July 2018 to “curb” online gossip.

Additionally, in 2017, the UCC issued a public notice advising the “general public against irresponsible and/or illegal use of all communication platforms.” The notice also called for users, administrators, and account managers to avoid “authoring, posting, receiving, and sharing or forwarding any forms of communication containing and/or referring to illegal and/or offensive content to avoid the risk of being investigated and/or prosecuted for aiding and abetting the commission of any resultant offenses.” ¹ The notice continued the government's practice of attempting to control and constrain social and political discourse on social media platforms.

In the past, the UCC has also banned media outlets from live-broadcasting parliamentary proceedings. In 2017, for example, the UCC banned live broadcasts of debates on the constitutional amendment bill that sought to lift the presidential age limit of 75, which would allow President Museveni to potentially remain in office for life. The UCC claimed that the broadcasts were likely to incite violence. ² However, some media houses bypassed the ban and live broadcast the proceedings via Twitter’s Periscope. The ban was lifted later in 2017, but with the condition that media houses possess “live broadcasting preediting software.” ³

Online disinformation campaigns are a growing issue in Uganda, though their influence has not been as pervasive as in other countries, such as Kenya. Research on social media trends during the 2016 elections found that automatically generated Twitter bots mimicking human users worked to manipulate online conversations by skewing discussions in favor of incumbent candidate President Museveni, leading to suspicions of paid progovernment trolling. ⁴

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

2 / 3

During the coverage period, there were new economic and regulatory constraints that negatively affected users’ ability to publish content online. The OTT tax instituted in July, for example, created a new economic barrier for those seeking to publish on social media or other communications platforms (see A2).

In March 2018, the UCC issued a directive requiring “all online data communication service providers, including online publishers, online news platforms, online radio and television operators” to obtain the UCC’s authorization to operate.” ¹ As part of the registration requirements, online publishers are required to pay \$20 per year. ² Observers noted that the directive strengthened the UCC’s powers to limit online speech, though it remains unclear how the registration requirements will apply to

content hosted outside Uganda. Communications service providers were given a deadline of April 2 to register or face blocking. Only 14 local blogs and news sites had registered by the deadline, prompting the UCC to issue another directive on April 19 (see B3). This authorization regulation was the justification for the UCC's attempt to shut down the *Daily Monitor's* website in February 2019 (see B3). ³ In August 2019, after the coverage period, the Ugandan Communication Commission moved forward with enforcing the registration program. ⁴

B7 0-4 pts

Does the online information landscape lack diversity?	3 / 4
--	--------------

Content available online in Uganda is somewhat diverse, though news websites published by the Vision Group, a media company that is partly owned by the government, are only available in four local languages (out of 40 languages and 56 indigenous dialects). Newspapers such as *Bukedde*, *Etop*, *Rupiny*, and *Orumuri* have created online platforms. Other news sites of major privately owned newspapers are only accessible in English, which is not widely spoken across Uganda. The Google Uganda domain is available in five local languages, ¹ while the Firefox web browser can be accessed in two languages, Luganda and Acholi. ² Wikipedia can be accessed in Luganda, with approximately 1,000 articles translated. ³

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	4 / 6
--	--------------

Vibrant digital activism continued to help raise awareness and mobilize citizens on issues including cybercrime, social injustices, and violations of internet freedom during the reporting period. Online mobilization tools are available to users.

In August 2018, the #FreeBobiWine social media campaign drew international attention following the arrest of Robert Kyagulanyi (better known as Bobi Wine), an opposition member of Parliament, along with fellow opposition Parliament member Kassiano Wadri and 32 others, while campaigning for Wadri in Arua. ¹ Wine and Wadri were later released, but still faced criminal charges at the end of the reporting period. ²

In July 2018, following the introduction of the social media tax, Ugandans took to social media using the hashtags #SocialMediaTax, #MobileMoneyTax, and #ThisTaxMustGo to urge the government to abolish the tax. The social media tax also attracted international attention, mobilizing internet stakeholders around the #NoToSocialMediaTax campaign to place further pressure on the government. Despite significant activism, the tax remained in effect as of the end of the coverage period. ³

In March 2018, the Nation Media Group–Uganda launched the online campaign #StayinYourLane, which published photographs and videos of errant drivers in an effort to curb unsafe driving. ⁴ The campaign led to the arrest of a police officer for violating traffic laws. ⁵

C. Violations of User Rights

As in past years, several individuals were arrested for their online speech during the coverage period. In February 2019, the UCC issued a warning threatening prosecution for those who publish fake news online. New reporting by the Wall Street Journal revealed close cooperation on national security and policing between the Ugandan government and Huawei, a Chinese technology company. In March 2019, the UCC called for the reregistration on SIM cards.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?

2 / 6

The Ugandan constitution provides for freedom of expression and speech, in addition to the right to access information and privacy. However, several laws undermine these protections.

Laws including the 2000 Press and Journalist Act, sections of the 1950 Penal Code Act, and the 2002 Anti-Terrorism Act appear to negate these constitutional guarantees for freedom of expression. For example, the Press and Journalist Act requires journalists to register with the statutory Media Council, whose independence is believed to be compromised by the government's influence over its composition.

Several court cases related to online freedom of expression are still open with no known hearing dates set, with the lead plaintiffs expressing frustration about the neglect of the cases by the judiciary. ¹

The independence of the Ugandan judiciary has become more tenuous in recent years. ² As part of his efforts to consolidate power in the run-up to the 2016 elections, the president promoted new judges to both the Constitutional Court and the Supreme Court in 2015. The process was criticized for lacking transparency and undermining judicial independence, while other critics called for more public scrutiny in the appointment of new judges. ³

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?

2 / 4

Several laws criminalize legitimate online expression and activities, including the Penal Code, the 2011 Computer Misuse Act, the 2014 Anti-Pornography Act, and the Anti-Terrorism Act.

The Penal Code contains provisions on criminal libel and the promotion of sectarianism, which are punishable with lengthy prison terms. While none of these laws contain specific provisions on online expression, they could be invoked for digital communications.

The 2011 Computer Misuse Act includes provisions that can specifically limit freedom of expression online. Under Section 25 of the law, the dissemination of “offensive communication” is prohibited alongside child pornography and cyberharassment, and is vaguely defined as the use of “electronic communication to disturb or attempts to disturb the peace, quiet, or right of privacy of any person.” Offenses under this provision of the act are considered misdemeanors and those convicted are subject to fines, imprisonment of up to one year, or both. ¹ In 2017, Unwanted Witness Uganda and the Uganda Human Rights Enforcement Foundation petitioned the Constitutional Court to challenge the constitutionality of Section 25 and “its failure to meet regional and international human rights norms and standards.” ² As of May 2019, the case was still ongoing. ³

The 2002 Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, which is vaguely defined, and convictions can carry the death sentence. ⁴ Amendments to the act adopted in 2015 may impact internet freedom in its broad criminalization of the “indirect” involvement in terrorist activities and the “unlawful possession of materials for promoting terrorism, such as audio or videotapes or written or electronic literature.” ⁵

The 2014 Anti-Pornography Law threatens to hold service providers criminally liable for the uploading or downloading of vaguely defined pornographic material on their systems, ⁶ with penalties of up to five years in prison and fines of \$4,000.

C3 0-6 pts

Are individuals penalized for online activities?	3 / 6
---	--------------

During the coverage period, the government continued to curtail free speech online by prosecuting voices of dissent, and a number of individuals who criticized the government and President Museveni on social media faced criminal charges.

In October 2018, Suzan Namata was arrested and charged under the Computer Misuse Act for offensive communication and harassing the

president, for posting a video that circulated on social media condemning the continued detention of an opposition leader. Namata's case was ongoing at the end of the reporting period. In February 2019, the police interrogated well-known socialite Shanita Namuyimbwa, better known as Bad Black, for insulting a senior government official in a video shared in August 2018, which criticized the arrest and detention of Bobi Wine. ¹ The socialite was investigated for offensive communication and criminal libel under the Computer Misuse Act and the Penal Code Act, respectively.

In November 2018, prominent academic and government critic Stella Nyanzi was arrested and jailed on separate charges of cyberharassment and offensive communication, for allegedly insulting the president and his mother in a Facebook post. ² In August 2019, after the coverage period, Nyanzi, who had already been jailed for nine months, was sentenced to an additional nine months in prison after being found guilty by a court. ³

Users are also penalized for pornographic content, which is illegal in Uganda. In June 2018, the Pornography Control Committee announced that it would arrest six individuals for sharing pornography. ⁴ Among those arrested was Lillian Rukundo, a 23-year-old student who was charged with 10 counts of broadcasting pornographic material and jailed in July 2018. ⁵

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	2 / 4
--	-------

There are no known restrictions on data encryption in Uganda. However, anonymous communication is compromised by mandatory registration for SIM cards and mobile internet subscriptions. The 2015 Registration of Persons Act requires all citizens to use national identification cards for SIM card registration. In March 2019, the UCC directed all mobile providers to reregister SIM cards. This followed a large-scale registration exercise carried out in March 2018, when the UCC directed telecommunications companies to cease the sale of SIM cards until it

could directly access the National Identification and Registration Authority (NIRA) database. ¹ The directive was ostensibly aimed at curbing crime being perpetrated through the use of unregistered SIM cards. The ban on selling new SIM cards was lifted in May 2018, with stricter guidelines for registering, upgrading, or replacing a SIM card. SIM card applicants are now required to physically present an original national identification card or, for non-Ugandans, a passport, to an operator's designated customer care agent. ² The operator is then required to verify the authenticity of the national identification card using an electronic biometric card reader, and obtain real-time verification using the NIRA database. Additionally, if operators fail to conduct online real-time verification, they are required to deny the issuance, upgrade, or replacement of SIM cards. ³

The UCC's requirement for online publishers, vaguely defined as "data communicators," to register raises concerns about anonymity, as it may limit the anonymity of bloggers and social media influencers (see B6).

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	2 / 6
--	--------------

Many activists have expressed suspicions that the government has increased monitoring and surveillance of social media platforms and other online spaces in recent years. The 2019 Data Protection and Privacy Act

¹ was signed by President Museveni in February 2019, following a civil society push for the law. The law provides for the protection of privacy and the security of personal data by regulating the collection and processing of personal information in Uganda.

Despite the law, significant concerns about government surveillance persist. ² State authorities have admitted to publicly monitoring social media posts. In March 2019, during Stella Nyanzi's trial, a security officer testified about actively monitoring her Facebook page. ³ In 2017, the Uganda Media Centre, the government-appointed media regulatory body, publicly announced that it had implemented a new social media

monitoring unit that scans the profiles of social media users to find critical posts. ⁴

The government's surveillance powers are governed by the 2010 RIC Act, which was hurriedly passed following the 2010 al-Shabaab terrorist attack in Kampala, Uganda. Under the RIC Act, telecommunications companies are required to install equipment that enables real-time electronic surveillance of suspected terrorists. The RIC Act also gives the security minister the ability to request access to personal communications based on national security concerns, ⁵ which can be granted following an order by a High Court judge. ⁶

In addition to the RIC Act, clauses in the 2002 Anti-Terrorism Act give security officers, appointed by the interior minister, the power to intercept communications of individuals suspected of terrorism and to keep them under surveillance, without judicial oversight. ⁷

In a 2018 report by Citizen Lab, a Canadian internet watchdog, Uganda is listed as one of 45 countries worldwide using Pegasus, a targeted spyware software developed by the Israeli technology firm NSO. Pegasus is known to be used by governments to spy on journalists, human rights defenders, and the opposition. ⁸

An article published by the *Wall Street Journal* in August 2019, after the coverage period, revealed close cooperation between the Ugandan government and Huawei, a Chinese technology company, to surveil opposition figures and government critics. The Ugandan government confirmed that the police and intelligence services work with Huawei on national security issues, including by using spyware against "security threats and political enemies." Huawei employees working in Kampala's police headquarters allegedly helped the Ugandan police surveil Bobi Wine by using spyware to access a WhatsApp chat group. In July 2018, construction began on Huawei's "safe city" project in Uganda, which includes the installation of CCTV cameras across the country and the implementation of a facial recognition surveillance system, raising further concerns about government surveillance and Huawei's role in aiding the government in the monitoring of its citizens. ⁹

In 2017, the *Daily Monitor* reported on a new deal between the governments of China and Uganda, in which the Chinese government would provide assistance in developing a comprehensive cybersecurity strategy for Uganda, including the “technical capacity to monitor and prevent social media abuse.” ¹⁰ No further information about the technology and its potential implementation has surfaced to date.

The government has been known to surveil critics and opponents in the past, according to research by Privacy International (PI). In a 2015 report, PI detailed a secret government operation that involved implanting FinFisher intrusion malware on the Wi-Fi networks of several hotels in Kampala, Entebbe, and Masaka to illegally spy on targeted activists, opposition politicians, and journalists between 2011 and 2013. ¹¹ It is unclear whether FinFisher was still being deployed during this report’s coverage period.

A raid on MTN’s offices by Uganda’s Internal Security Organization, a domestic intelligence unit, in July 2018 raised concerns about the security of user data. ¹²

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	3 / 6
---	--------------

Service providers and other technology companies are required to retain metadata for an unspecified amount of time. ¹ Under the RIC Act, providers are also required to disclose the personal information of individuals suspected of terrorism or considered a threat to national security, public safety, or national economic interests, to the authorities, upon issuance of a warrant or notice from the security minister. ² Failure to comply with the provisions in the RIC Act can result in five years in prison for intermediaries, in addition to license revocations. ³ It is unclear to what extent these provisions have been implemented or operationalized.

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

3 / 5

Media freedom continues to decline as a result of government harassment and intimidation of journalists. In February 2019, the UCC issued a warning that threatened prosecution for publishers of fake news online. ¹ The warning followed a post widely circulated on social media that attributed a call for the ban of a politically controversial song to the executive director of the UCC.

The last reported instance of violence for online activities occurred in 2017, when NTV Uganda news anchor Gertrude Uwitware was abducted by unknown assailants and badly beaten following posts she made on her blog defending academic Stella Nyanzi's criticisms of the current regime (see C3). The government is known to bar media outlets from reporting on opposition activities and harass journalists believed to be reporting for the opposition. ² The government has also been accused of "fostering a climate of fear and paranoia" among journalists for failing to investigate a series of break-ins of media houses, which resulted in the theft of journalists' computers in 2017. ³

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?

2 / 3

Hacking and cyberattacks were less prevalent during the reporting period, but some incidents threatened online security. During the coverage period, a Ministry of Labor external recruitment database was hacked and sensitive external recruitment data was stolen. ¹ The hack was purportedly perpetrated by a ministry official in "collusion with unscrupulous labor recruitment agencies to get undue clearance for their domestic workers."

The state has been known to target critics and opponents with surveillance malware, according to research published by Privacy International in 2015, which detailed a secret government operation that implanted FinFisher intrusion malware on the Wi-Fi of several hotels to illegally spy on activists, opposition politicians, and journalists between 2011 and 2013 (see C5). ² It is unclear whether these technical attacks were still being deployed during the coverage period.

Vulnerable populations and marginalized communities, particularly the LGBT+ community, have also been the target of regular technical attacks over the past few years. In 2016, the email and Facebook accounts of a social worker at the Most at Risk Populations Initiative were hijacked. ³ Activists believe the attack may have been perpetrated by the government, given the wealth of information the social worker possessed about the LGBT+ community through their work and private communications. Hacking attacks against gay individuals for the purpose of blackmail have also been reported. In one incident detailed in a 2016 interview, after the Facebook account of a closeted gay celebrity was hacked, screenshots of private messages pointing to his sexual orientation were used to blackmail him. ⁴



On Uganda

See all data, scores & information on this country or territory.

[See More >](#)

Country Facts

Global Freedom Score

34/100 Not Free

Internet Freedom Score

56/100 **Partly Free**

Freedom in the World Status

Not Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

No

Pro-government Commentators

No

Users Arrested

Yes*In Other Reports*[Freedom in the World 2019](#)*Other Years*

**Be the first
to know
what's
happening.**

Email

Join the Freedom
House monthly
newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org

@2021 FreedomHouse