Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2016 Cycle for Uganda

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world – including presence in the African Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes good security policies that protect user rights, including privacy and freedom of expression. Access Now has worked extensively in Africa on digital rights including commenting on the establishment of the African Union Convention on Cyber Security and Personal Data Protection ("the Convention"). We now welcome the opportunity to provide feedback on the Universal Periodic Review 2016 Cycle for Uganda.
3. This is the second review for Uganda, last reviewed in October 2011 where the Ugandan government voluntarily accepted and pledged to implement 170 recommendations in the area of human rights during the review at the Universal Periodic Review Mechanism (UPRM) in Geneva. However, an Inter-ministerial meeting held on February 23rd, 2012 in Kampala and chaired by the Ministry of Foreign Affairs rejected 21 recommendations out of 42 which had been not been formally accepted by the same government during the October 2011 Geneva review.

Domestic and international human rights obligations

4. Uganda has signed onto various international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR), the Convention against Torture (CAT), the Convention against Enforced Disappearance (ICCPED), and the Optional Protocol to the CAT (OPCAT).
5. Article 29(1)a, Article 41(1), Article 20(1) of the 1995 Constitution of Uganda provide protections for freedom of expression and speech, in addition to the right of access to information.
6. Despite these above provisions, several laws—including the Press and Journalist Act, sections of the penal code, and the Anti-Terrorism Act—are vague enough to be used to violate constitutional guarantees for freedom of expression.

Situation of digital rights in Uganda

7. Despite these commitments and obligations, we have gathered and hereby submit evidence of a systematic disregard of digital rights in Uganda. These violations include:

Violations of access to information & freedom of expression

8. On February 18, 2016 Ugandan internet users detected an internet outage affecting Twitter, Facebook, and other communications platforms.[1] According to the Uganda Communications Commission (UCC), blocking was carried out on orders of the Electoral Commission, for security reasons.[2] The shutdown coincided with voting for the presidential election, and remained in place until the afternoon of Sunday, February 21. During this period, two presidential candidates were detained under house arrest.[3] The telco MTN Uganda confirmed the UCC directed it to block "Social Media and Mobile Money services due to a threat to Public Order & Safety."[4] The blocking order also affected the telcos Airtel, Smile, Vodafone, and Africel. President Museveni admitted to journalists on February 18 that he had ordered the block because "steps must be taken for security to stop so many (social media users from) getting in trouble; it is temporary because some people use those pathways for telling lies."[5]
9. The international community labels this type of blocking of telecommunications networks and services as an "internet shutdown."[6] Research shows that internet shutdowns and human rights infringements go hand-in-hand.[7] Shutdowns disrupt the free flow of information and create a cover of darkness that allows state and non-state actors to persecute vulnerable groups without scrutiny. They also drastically harm the economy -- in the case of Uganda, by impacting mobile money transfers.
10. A growing body of jurisprudence declares shutdowns to violate international law. In 2015, various experts from the United Nations (UN) Organization for Security

---

[1] Omar Mohammed, 'Twitter and Facebook are blocked in Uganda as the country goes to the polls' (Quartz Africa, 18 February 2016) <http://qz.com/619188/ugandan-citizens-say-twitter-and-facebook-have-been-blocked-as-the-election-gets-underway/> accessed 18 February 2016.

[2] Uganda blocks social media for 'security reasons', polls delayed over late voting material delivery (The Star, 18 February 2016) <http://www.the-star.co.ke/news/2016/02/18/uganda-blocks-social-media-for-security-reasons-polls-delayed-over_c1297431> accessed 18 February 2016.

[3] Brian Duggan, "Uganda shuts down social media; candidates arrested on election day" (CNN, 18 February 2016) <http://www.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/> accessed 22 February 2016.

[4] MTN Uganda <https://twitter.com/mtnug/status/700286134262353920> accessed 22 February 2016.

[5] Tabu Batugira, "Yoweri Museveni explains social media, mobile money shutdown" (Daily Nation, February 18, 2016) <http://www.nation.co.ke/news/Yoweri-Museveni-explains-social-media-mobile-money-shutdown/-/1056/3083032/-/8h5ykhz/-/index.html> accessed 22 February 2016.

[6] "Fighting Internet Shutdowns" (Access Now) <https://www.accessnow.org/internet-shutdowns>

[7] Sarah Myers West, 'Research Shows Internet Shutdowns and State Violence Go Hand in Hand in Syria' (Electronic Frontier Foundation, 1 July 2015) <https://www.eff.org/deeplinks/2015/06/research-shows-internet-shutdowns-and-state-violence-go-hand-hand-syria> accessed 18 February 2016.

and Co-operation in Europe (OSCE), Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR), issued an historic statement declaring that internet "kill switches" can never be justified under international human rights law, even in times of conflict.[8] General Comment 34 of the UN Human Rights Committee, the official interpreter of the International Covenant on Civil and Political Rights, emphasizes that restrictions on speech online must be strictly necessary and proportionate to achieve a legitimate purpose. Shutdowns disproportionately impact all users, and unnecessarily restrict access to information and emergency services communications during crucial moments.

11. The internet has enabled significant advances in health, education, and creativity, and it is now essential to fully realize human rights including participation in elections and access to information. Shutdowns and blocking of internet services delay and deter the benefits of these advances and economic development more broadly.

Additional legal provisions that violate the freedom of expression

12. The Press and Journalist Act of 2000 requires journalists to register with the statutory Media Council. This is a body whose independence is compromised by the government's influence over its composition. Moreover, journalism is a function, and those engaging in journalistic activities should not be required to obtain a license for their work. The Human Rights Committee has found that "general State systems of registration or licensing of journalists are incompatible" with Article 19.[9]
13. Additionally, the penal code contains provisions on criminal libel and the promotion of sectarianism, imposing penalties that entail lengthy jail terms. These provisions are vague and overbroad, and create a "chilling effect" on freedom of expression both online and offline.
14. Similarly, the 2002 Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, which is vaguely defined. Such vague terms as "indirect" involvement in terrorist activists and the "unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature" do not clearly delineate which behaviors are prohibited. Despite the uncertain application of these provisions, the penalties for non-compliance are very severe, as convictions can carry the death sentence.[10]
15. Under Act 2 of the 2011 Computer Misuse Act includes provisions that can specifically limit freedom of expression online. The law prohibits the dissemination of "offensive communication" alongside child pornography and cyber harassment, 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."

---

[8] Peter Micek, (Access Now 4 May 2015) 'Internet kill switches are a violation of human rights law, declare major UN and rights experts' <https://www.accessnow.org/blog/2015/05/04/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un> accessed 18 February 2016.

[9] Human Rights Committee, General Comment No. 34 <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

[10] Art.9 (b), The Anti-Terrorism Act, 2002 <http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf >

Violations of the right to privacy

16. In July 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the Ugandan government had began looking into purchasing the company's sophisticated spyware known as Remote Control System (RCS) from April 2015.[11] These systems are often used by governments for unlawful surveillance, including to target and arrest human rights defenders around the world.
17. Through the 2010 Regulation of Interception of Communication (RIC) Act, telecommunication companies are required to install equipment that enables real-time electronic surveillance of suspected terrorists. Such equipment enables unlawful and arbitrary surveillance of law-abiding internet users and its use must be strictly circumscribed. The RIC Act also gives the government permission to tap into personal communications for national security concerns.[12] Orders can be requested by security minister and granted after an order by a High Court judge.[13]

Recommendations

18. Uganda can improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of Uganda:
    a. Commit to acting upon the resolution on democracy in the digital era of October 21, 2015, which took place during the 133rd Assembly of the Inter-Parliamentary Union (IPU). Uganda was among the 167 national governments that unanimously adopted the resolution;
    b. Commit to enhancing freedom of expression online and preventing violations by state and non-state actors, such as companies;
    c. Commit to refrain from slowing, blocking, or shutting down internet and telecommunications services, particularly during elections and public assemblies;
    d. Publicly disclose any procurement of or contracts to purchase, maintain, or operate surveillance technology;
    e. Improve cooperation with United Nations and African Union treaty mechanisms and issue standing invitations to UN special procedures such as the UN special rapporteurs on freedom of expression and privacy; and
    f. Enact laws protecting access to information and preventing network discrimination, also known as Net Neutrality.
19. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.

---

[11] Mujuni Raymond Qatahar, "Wikileaks Emails: Uganda To Buy 3bn Surveillance Equipment," *Qataharray* (blog), July 21, 2015, <https://qataharray.wordpress.com/2015/07/21/wikileaks-emails-uganda-to-buy-surveillance-equipment/ >

[12] Amnesty International, "Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act, 2010," December 14, 2010, <https://www.amnesty.org/en/documents/AFR59/016/2010/en/ >

[13] See , Regulation of Interception of Communications Act, 2010 Section 5

20. For additional information, please contact Access Now staff Ephraim Percy Kenyanito (ephraim@accessnow.org) and Peter Micek (peter@accessnow.org).