Submission to the United Nations Human Rights Council on the Universal Periodic Review 33rd Session for Ethiopia

About

Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the protection of fundamental rights and the internet's continued openness. Access Now engages through an action-focused global community, and Technology Arm operating a 24/7 digital security helpline.

Small Media (www.smallmedia.org.uk) is a UK-based organisation that works to support the free flow of information in closed societies through training, research and technology. Small Media works with local partners across the Middle East and Sub-Saharan Africa to support their efforts to advance internet freedom, and defend human rights online. It engages in research to identify the development needs of partners and priorities for policy advocacy. It also provides targeted trainings and technology support to help local partners influence policy, and safeguard their communities from digital threats.

Domestic and international human rights obligations

1. Ethiopia has ratified the International Covenant on Civil and Political Rights ("ICCPR"), the International Covenant on Economic, Social, and Cultural Rights ("ICESCR").
2. Article 26 of the Constitution of the FDRE covers the right to privacy. In it, it specifically states that every person has the right to the inviolability of communications made by phone, telecommunications, and electronic devices.
3. Article 29 of the Constitution protects both the right to freedom of expression and right to information without interference. In a later point, it also protects the freedom of the press, specifically prohibiting any form of censorship and ensuring access to information of public interest.

Developments of digital rights in Ethiopia

4. Recently, positive reforms in internet freedom and digital rights have swept through Ethiopia. Over the past decade, the government has dropped the charges against many bloggers,[1] journalists,[2] and opposition groups,[3] and has

[1] https://www.news24.com/Africa/News/ethiopia-drops-charges-against-zone-9-bloggers-20180214

[2] https://www.amnesty.org.au/ethiopian-journalist-eskinder-nega-released-prison/

freedom thousands of prisoners.[4] On June 22, 2018, it was announced that the government has unblocked 264 websites and TV broadcasters.[5] The recent internet shutdown in August 2018, however, quells the hope created by these improvements, and shows that Ethiopia still needs much improvement around protecting freedom of expression and access to information.

Violations of access to information & freedom of expression

5. The national government has shut off broadband and mobile internet amidst growing tensions between national and regional governments in Ethiopia. In August 2018, the cities of Harar and Dire Dawa and the whole Somali region of Ethiopia went without internet access for 22 days.[6]
6. Again, in September 2018, authorities shut down mobile internet in the capital amidst protests.[7]
7. These recent disruptions are the newest addition to a troubling history of implementing internet shutdowns. These shutdowns usually follow a controversial political event, such the complete shutdown of internet services during widespread anti-government protests on August 6 and 7, 2016, and the shutdown of mobile internet in 2017 from May 30 to June 8 following the conviction of two human rights activists.[8] Research and history show that internet shutdowns and state violence go hand-in-hand, making this pattern extremely concerning.[9]
8. Shutdowns are not constrained to the political realm; the Ethiopian government is also one of several countries known to block the internet during school exams.[10] This often involves cutting access throughout an entire region, or sometimes country, disconnecting businesses, emergency workers, hospitals, and governmental agencies, all for fear of cheating on a school exam.[11]
9. The Computer Crime Proclamation of 2016 criminalized an array of online activities, creating concern over its ability to censor critical commentary and political opposition. It criminalizes content that "incites fear, violence, chaos, or

[3] https://www.news24.com/Africa/News/top-ethiopian-dissident-bekele-gerba-freed-from-jail-20180214

[4] https://www.aljazeera.com/indepth/opinion/abiy-ahmed-transforming-ethiopia-face-adversity-180622112645741.html

[5] https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites/

[6] https://www.accessnow.org/ethiopia-blocks-internet-in-eastern-part-of-country-again/

[7] https://globalvoices.org/2018/09/20/netizen-report-authorities-shut-down-mobile-internet-in-ethiopias-capital-as-ethnic-and-political-conflict-persist

[8] https://freedomhouse.org/report/freedom-net/2017/ethiopia

[9] https://www.accessnow.org/joint-letter-uganda-social-media-blackout/

[10] http://www.africanews.com/2018/03/21/unexplained-internet-blackout-in-ethiopia-s-oromia-region//

[11] https://www.accessnow.org/need-stop-shutting-internet-school-exams/

conflict among people" and bans the dissemination of defamatory content," punishing both acts with years of jail time.[12]

Violations of the right to privacy

10. The Computer Crime Proclamation of 2016 strengthened government surveillance of online and mobile phone communications as well. The act enabled real-time monitoring or interception of communications, authorized by the Minister of Justice, and commands service providers to store records of all communications and metadata for at least a year.[13]
11. There are strong indications that the government has implemented two surveillance products developed by Chinese telecommunications firm, ZTE. The first is a centralized monitoring system, designed to monitor mobile phone networks and the internet. This system, known for its use by regimes in Libya and Iran, enables deep packet inspection of internet across the EthioTelecom network and can intercept emails and online messaging.[14] EthioTelecom has also installed ZSmart, a customer management database that is also developed by ZTE. ZSmart manages all aspects of a customer's account and provides full access to user information and the ability to intercept SMS text messages and record phone conversations. Phone call information includes the originating and receiving phone numbers, the location of originator/receiver, and the time, date, and duration of every call. [15]
12. In 2015, Citizen Lab released a report suggesting that the Ethiopian Information Network Security Agency (INSA) was involved in an attempted hacking of several Washington DC-based journalists with the Ethiopian Satellite Television Service (ESAT). They also noted that this attacker seemed to be the same entity as the one that targeted ESAT journalists in Belgium and US in 2013. The reporters were attacked by what appeared to be Hacking Team's Remote Control System (RCS) spyware, and the attacker was linked to Ethiopia. The second attack is especially notable because it suggests that the same attacker, using updated Hacking Team software, continued in its malicious efforts even after the first attack had been widely reported and condemned.[16]

[12] https://freedomhouse.org/report/freedom-net/2017/ethiopia

[13] https://freedomhouse.org/report/freedom-net/2017/ethiopia
http://hornaffairs.com/en/2016/05/09/ethiopia-computer-crime-proclamation/

[14]
https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia
https://freedomhouse.org/report/freedom-net/2017/ethiopia

[15] https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

[16] https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/#2

13. Inside Ethiopia, many people are so convinced of the government's surveillance practices that they self-censor when using technology to communicate. According to many interviews made in a Human Rights Watch report, individuals only use the phone to make appointments with no substantive conversation taking place, use fake email addresses, and avoid using certain sensitive keywords.[17]

Recommendations

14. The government should amend the Computer Crime law so that it adheres to international standards and preserves the privacy rights of citizens.
15. The government must halt all unlawful and unwarranted large-scale surveillance of citizens and targeted surveillance of activists, journalists, and dissenting voices.
16. The government should not shut down or disrupt access to the internet, SMS, or other landline or mobile communications networks and services. Rather, the government should comply with Art. 19 of the ICCPR, as interpreted by General Comment 34, and UN resolutions that condemn such intentional disruptions, including A/HRC/RES/38/7 and A/HRC/RES/38/11. Any laws and regulations allowing shutdowns should be reformed to comply with international law.
17. The Ethiopian government should introduce a robust data protection law that protects the privacy and security of Ethiopians.
18. 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 and Small Media are grateful to make this submission.

Contact information:

Access Now
Peter Micek
Email: peter@accessnow.org
Web: https://www.accessnow.org

Small Media
James Marchant
Email: james@smallmedia.org.uk
Web: https://smallmedia.org.uk

[17] https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

accessnow