

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	328
Land:	Etiopien
Kilde:	Freedom House
Titel:	Freedom on the Net 2017 – Ethiopia
Udgivet:	14. november 2017
Optaget på baggrundsmaterialet:	29. januar 2018

Freedom on the Net 2017 - Ethiopia

Country:

Ethiopia

Year:

2017

Status:

Not Free

Total Score:

86

(0 = Best, 100 = Worst)

Obstacles to Access:

24

(0 = Best, 25 = Worst)

Limits on Content:

30

(0 = Best, 35 = Worst)

Violations of User Rights:

32

(0 = Best, 40 = Worst)

Population:

102.4 million

Internet Penetration:

15.4 percent

Social Media/ICT Apps Blocked:

Yes

Political/Social Content Blocked:

Yes

Bloggers/ICT Users Arrested:

Yes

Press Freedom Status:

Not Free

Key Developments:

June 2016–May 2017

Internet and mobile phone networks were deliberately disrupted during antigovernment protests and student exams; social media and communications platforms were periodically blocked throughout the year (see Restrictions on Connectivity and Blocking and Filtering).

Self-censorship heightened following the state of emergency instituted in October 2016 (see Media, Diversity, and Online Manipulation).

The state of emergency eroded fundamental rights and restricted certain online activities, including supporting protests on social media (see Legal Environment).

The Computer Crime Proclamation enacted in June 2016 criminalizes online defamation and incitement and strengthened the government's surveillance capabilities by enabling real-time monitoring or interception of communications (see Legal Environment and Surveillance, Privacy, and Anonymity).

Numerous individuals were arrested for online speech or protests; two were convicted and handed multi-year prison sentences (see Prosecutions and Detentions for Online Activities).

Introduction:

Internet freedom declined dramatically in the past year as the government imposed emergency rule to crack down on antigovernment protests and the digital tools citizens used to organize them.

The authoritarian government declared a six-month state of emergency in October 2016 following months of escalating protests. Starting in the Oromia region in November 2015 as a protest against the government's plan to infringe on land belonging to the marginalized Oromo people, the protests spread across the country throughout 2016, turning into unprecedented demonstrations seeking regime change and democratic reform. Emergency rule derogated fundamental rights in violation of international standards,¹ banned unauthorized protests, and allowed the authorities to arbitrarily arrest and detain citizens without charges. More than 21,000 people were arrested before the state of emergency was lifted in August 2017.

The state of emergency restricted certain online activities and the internet was shut down for several days. The authorities criminalized accessing or posting content related to the protests on social media, displaying antigovernment symbols or gestures, as well as efforts to communicate with "terrorist" groups—a category that includes exiled dissidents. Penalties included prison terms of between three and five years.

Numerous individuals were arrested for online activities, and two were convicted to long prison sentences. In May 2017, a prominent opposition activist, Yonatan Tesfaye, was sentenced to six and a half years in

prison on terrorism charges based on Facebook posts in which he criticized the government's handling of the Oromia protests. Also in May, Getachew Shiferaw, editor-in-chief of opposition outlet Negere Ethiopia, was sentenced to one and a half years in prison on subversion charges for Facebook comments published in support of an exiled journalist. He was released on time served.

The legal environment for internet freedom became more restrictive under the Computer Crime Proclamation enacted in June 2016, which criminalizes defamation and incitement. The proclamation also strengthens the government's surveillance capabilities by enabling real-time monitoring or interception of communications.

Obstacles to Access:

Internet and mobile phone networks were deliberately disrupted during antigovernment protests and student exams throughout the year. Meanwhile, poor infrastructure, obstructionist telecom policies, and a government monopoly on the information and communication technology (ICT) sector make ICT services prohibitively expensive for the majority of the population.

Availability and Ease of Access

Ethiopia is one of the least connected countries in the world with an internet penetration rate of only 15 percent in 2016, up from 12 percent the previous year, according to the latest data from the International Telecommunications Union (ITU).² Mobile phone penetration is also low at 51 percent, up from 43 percent in 2015.³ Low penetration rates stem from underdeveloped telecommunications infrastructure, which is almost entirely absent from rural areas, where about 85 percent of the population resides. A handful of signal stations service the entire country, resulting in network congestion and frequent disconnection.⁴ In a typical small town, individuals often hike to the top of the nearest hill to find a mobile phone signal.

Access to ICT services remains prohibitively expensive for most Ethiopians, largely due to the government's monopoly over the telecom sector, which provides consumers with few options. Prices are set by state-controlled EthioTelecom and kept artificially high.⁵ William Davison, Bloomberg's Ethiopia correspondent, described the issue on Facebook in March 2016: "It cost me 44 birr (\$2.05) to watch Al Jazeera's latest 3-minute dispatch on Oromo protests using 4G network on my phone, which is not that much less than the average daily wage of a daily laborer in Ethiopia."⁶ Ethiopians can spend an average of US\$85 per month for limited mobile or fixed wireless internet access. Better quality services in neighboring Kenya and Uganda cost less than US\$30 a month. One comparative assessment of internet affordability put Ethiopia among the world's most expensive countries for access.⁷

Telecommunication devices, connection fees and other related costs are also beyond the means of many Ethiopians. As a result, Ethiopia has one of the lowest smartphone ownership rates in the world at only 4 percent, according to a 2016 Pew survey.⁸ Consequently, the majority of internet users rely on cybercafes for internet access. A typical internet user in the capital, Addis Ababa, pays between ETB 5 and 7 (US\$ 0.25 to 0.35) for an hour of access. Because of the scarcity of internet cafes outside urban areas, however, rates in rural cybercafes are higher. In addition, digital literacy rates are generally low.

Connection speeds have been painstakingly slow for years, despite the rapid technological advances improving service quality in other countries. According to Akamai, the average connection speed in Ethiopia

was 3 Mbps in the first quarter of 2017, significantly lower than the global average of 7.0 Mbps. In practice, such speeds result in extremely sluggish download times for even simple images. Logging into an email account and opening a single message can take as long as five minutes at a standard cybercafe with broadband in the capital, while attaching documents or images to an email can take eight minutes or more.⁹

Restrictions on Connectivity

Throughout 2016 and 2017, network traffic in and out of Ethiopia registered a significant decline as a result of continual throttling and repeated internet shutdowns.

Network shutdowns occurred several times during the coverage period:

During widespread antigovernment protests on August 6 and 7, 2016, internet services were completely inaccessible in the Amhara, Addis Ababa, and Oromia regions. The government responded to the protests with excessive force, resulting in the deaths of at least 100 people.¹⁰

In October 2016, mobile internet services were shut down for several days when the government declared a state of emergency.¹¹ Mobile internet service and social media remained intermittently accessible for months (see Legal Environment).

The government shut down all telecommunications networks from May 30 to June 8 following the conviction of two human rights activists for online expression in May 2017 (see Prosecutions and Detentions for Online Activities).¹²

In separate incidents in July 2016, August 2016, and June 2017, the authorities shut down fixed and mobile internet services in select regions to prevent students from cheating during national university exams.¹³

The ICT shutdowns were costly. According to October 2016 research by the Brookings Institution, network disruptions between July 1, 2016 and June 30, 2017 cost Ethiopia's economy over USD \$8.5 million.¹⁴ September 2017 research by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) calculated the economic cost of Ethiopia's internet disruptions between 2015 and 2017 at nearly USD \$3.5 million a day. Calculated separately, disruptions to apps cost nearly USD \$875,000 a day.¹⁵

The Ethiopian government's monopolistic control over the country's telecommunications infrastructure via EthioTelecom enables it to restrict information flows and access to internet and mobile phone services. As a landlocked country, Ethiopia has no direct access to submarine cable landing stations; thus, it connects to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and the SEACOM cable that connects through Djibouti to an international undersea cable. All connections to the international internet are completely centralized via EthioTelecom, enabling the government to cut off the internet at will.

ICT Market

State-owned EthioTelecom holds a firm monopoly over internet and mobile phone services as the country's sole telecommunications service provider. Despite repeated international pressure to liberalize

telecommunications in Ethiopia, the government refuses to ease its grip on the sector.¹⁶ The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited.¹⁷

China is a key investor in Ethiopia's telecommunications industry,¹⁸ with Zhongxing Telecommunication Corporation (ZTE) and Huawei currently serving as contractors to upgrade broadband networks to 4G in Addis Ababa and expand 3G networks elsewhere.¹⁹ The partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector,²⁰ though the networks built by the Chinese firms have been criticized for their high cost and poor service.²¹ Furthermore, the contracts have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust ICT censorship and surveillance capacities (see Surveillance, Privacy, and Anonymity).²² In December 2014, the Swedish telecom group Ericsson also partnered with the government to improve and repair the mobile network infrastructure,²³ though ZTE remains the sector's largest investor.

Onerous government regulations also stymie other aspects of the Ethiopian ICT market. For one, imported ICT items are tariffed at the same high rate as luxury items, unlike other imported goods such as construction materials and heavy duty machinery, which are given duty-free import privileges to encourage investments in infrastructure.²⁴ Ethiopians are required to register their laptops and tablets at the airport with the Ethiopian customs authority before they travel out of the country, ostensibly to prevent individuals from illegally importing electronic devices, though observers believe the requirement enables officials to monitor citizens' ICT activities by accessing the devices without consent.²⁵

Local software companies also suffer from heavy-handed government regulations, which do not prescribe fair, open, or transparent ways of evaluating and awarding bids for new software projects.²⁶ Government companies are given priority for every kind of project, while smaller entrepreneurial software companies are completely overlooked, leaving few opportunities for local technology companies to thrive.

Cybercafes are subject to burdensome operating requirements under the 2002 Telecommunications (Amendment) Proclamation,²⁷ which prohibit them from providing Voice-over-IP (VoIP) services, and mandate that owners obtain a license from EthioTelecom via an opaque process that can take months. In the past few years, EthioTelecom began enforcing its licensing requirements more strictly in response to the increasing spread of cybercafes, reportedly penalizing Muslim cafe owners more harshly. Violations of the requirements entail criminal liability, though no cases have been reported.²⁸

Regulatory Bodies

The Ethiopian Telecommunications Agency (ETA) is the primary regulatory body overseeing the telecommunications sector. In practice, government executives have complete control over ICT policy and sector regulation.²⁹ The Information Network Security Agency (INSA), a government agency established in 2011 and controlled by individuals with strong ties to the ruling regime,³⁰ also has significant power to regulate the internet under its mandate to protect communications infrastructure and prevent cybercrime.

Limits on Content:

Social media and communications platforms were repeatedly blocked throughout the coverage period. Self-censorship heightened following the state of emergency instituted in October 2016, which placed restrictions on the use of social media for certain types of speech.

Blocking and Filtering

One of the first African countries to censor the internet,³¹ Ethiopia has a nationwide, politically motivated internet blocking and filtering apparatus that is reinforced during sensitive political events.

Tests conducted by the Open Observatory of Network Interference (OONI) in December 2016 found a wide range of websites blocked in Ethiopia, including the websites of Ethiopian news outlets known for critical reporting, political opposition groups, LGBTI (lesbian, gay, bisexual, transgender, or intersex) groups, human rights organizations, and circumvention tools. In total, at least one hundred websites were inaccessible.³² OONI tests also found the mobile version of WhatsApp completely blocked.³³

Other social media platforms such as Facebook and Twitter were repeatedly blocked for periods of time throughout 2016 and 2017, limiting their utility for political organizing even when the internet had not been completely shut down.³⁴ In one case unrelated to political unrest, the authorities also blocked access to Facebook, Twitter, Instagram, Viber, IMO, and Google+ to prevent cheating during university examinations in July 2016.³⁵ The blocks followed a full internet blackout for the same reason (see Restrictions on Connectivity). A government spokesperson stated that blocking social media during the exam would help students concentrate.

However, some progovernment media organizations and commentators seemed to have exclusive access to social media during the block,³⁶ which reinforced the popular belief that government supporters are not disadvantaged during shutdowns to the extent that citizens are. Tools that help internet users bypass censorship are frequently blocked in Ethiopia, but some may remain available for approved uses. When social media platforms were blocked in the past year, diaspora-based activists publicized virtual private networks (VPNs) to circumvent the censorship, but certain VPNs were also subsequently blocked.³⁷ Local sources suspected progovernment commenters were reporting some tools to the authorities for enabling censorship circumvention.

Digital security tools and information are also blocked. The Amharic translation of the Electronic Frontier Foundations' "Surveillance Self-Defense" web guide was blocked two weeks after it was published in October 2015.³⁸ One source reported that keywords such as "proxy" yield no search results on unencrypted search engines,³⁹ reflecting the government's efforts to limit users' access to proxy servers and other circumvention tools. Tor, a circumvention tool that enables users to browse anonymously, has been subject to restrictions since May 2012.⁴⁰

To filter the internet, specific internet protocol (IP) addresses or domain names are generally blocked at the level of the EthioTelecom-controlled international gateway. Deep packet inspection (DPI), which blocks websites based on a keyword in the content of a website or communication, is also employed.⁴¹

There are no procedures for determining which websites are blocked or why, precluding any avenues for appeal. There are no published lists of blocked websites or publicly available criteria for how such decisions are made, and users are met with an error message when trying to access blocked content. The decision-making process does not appear to be controlled by a single entity, as various government bodies—including the Information Network Security Agency (INSA), EthioTelecom, and the ICT ministry—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking. This lack of transparency is exacerbated by the fact that the government denies implementing censorship. Government

officials flatly deny blocking websites or jamming international satellite operations, while also stating that the government has a legal and a moral responsibility to protect the Ethiopian public from extremist content.

Content Removal

Political content is often targeted for removal, often by way of threats from security officials who personally seek out users and bloggers to instruct them to take down certain content, particularly critical content on Facebook. The growing practice suggests that at least some voices within Ethiopia's small online community are closely monitored. For instance, during antigovernment protests in Oromia, activists who wrote messages of solidarity for the protestors on Facebook were asked to delete their posts.⁴²

Media, Diversity and Content Manipulation

Increasing repression of journalists and bloggers has had a major chilling effect on expression online, particularly in response to the spate of blogger arrests in the past few years (see Prosecutions and Detentions for Online Activities). Many bloggers publish anonymously to avoid reprisals,⁴³ while fear of pervasive surveillance has also led to widespread self-censorship.

Self-censorship heightened during the state of emergency instituted in October 2016, which explicitly prohibited sharing information about protests through social media platforms, communicating with exiled dissident groups regarded as terrorists, organizing demonstrations, and displaying political gestures (see Legal Environment).

Lack of adequate funding is a significant challenge for independent online media in Ethiopia, as fear of government pressure dissuades local businesses from advertising with politically critical websites. A 2012 Advertising Proclamation also prohibits advertisements from firms "whose capital is shared by foreign nationals."⁴⁴ The process for launching a website on the local .et domain is expensive and demanding,⁴⁵ requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.⁴⁶ While the domestic blogosphere has been expanding, most blogs are hosted on international platforms or published by members of the diaspora.

Despite Ethiopia's extremely low levels of internet access, the government employs an army of trolls to distort Ethiopia's online information landscape.⁴⁷ Opposition groups, journalists, and dissidents use the mocking Amharic colloquial term *kokas* to describe the progovernment commentators.⁴⁸ Observers say the *kokas* regularly discuss Ethiopia's economic growth in favorable terms and post derogatory comments about Ethiopian journalists and opposition groups on Facebook and Twitter. In return, they are known to receive benefits such as money, land, and employment promotions. The government also manipulates online content through propaganda that aims to convince Ethiopians that social media is a dangerous tool co-opted by opposition groups to spread hate and violence.⁴⁹

Digital Activism

Online tools were essential for the mobilization of antigovernment protests throughout 2016, enabling activists to post information about the demonstrations and disseminate news about police brutality as the government cracked down on protesters.⁵⁰ Digital activism was muted following the October 2016 state of

emergency, which banned demonstrations and online mobilization. Repeated internet shutdowns and blocks on social media platforms also hindered mobilization efforts (see Blocking and Filtering and Restrictions on Connectivity).

Violations of User Rights:

A state of emergency declared in October 2016 derogated fundamental rights and restricted certain online activities. The Computer Crime Proclamation enacted in June 2016 criminalizes defamation and incitement; observers say it could be invoked to suppress digital mobilization. The proclamation also strengthens the government's surveillance capabilities by enabling real-time monitoring and interception of communications. Numerous individuals were arrested for online activities, particularly protests, while two people were sentenced to prison for several years each during the coverage period.

Legal Environment

The government imposed a six-month state of emergency in October 2016 and shut down the internet for several days to quell escalating antigovernment protests. Specific online activities were restricted under emergency rule.⁵¹ The authorities criminalized accessing or posting content related to the protests on social media, as well as efforts to communicate with "terrorist" groups, a category that includes exiled dissidents. Penalties included prison terms of three to five years.⁵² Emergency rule also undermined fundamental rights, banning unauthorized protests, and allowing the authorities to arbitrarily arrest and detain citizens without charge. More than 21,000 people were arrested before the state of emergency was lifted in August 2017, according to news reports.⁵³

Fundamental freedoms are guaranteed for Ethiopian internet users on paper, but the guarantees are routinely flouted in practice. The 1995 Ethiopian constitution provides for freedom of expression, freedom of the press, and access to information, while also prohibiting censorship.⁵⁴ These constitutional guarantees are affirmed in the 2008 Mass Media and Freedom of Information Proclamation, known as the press law, which governs the print media.⁵⁵ Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression, such as complex registration processes for media outlets and heavy fines for defamation.⁵⁶ The Criminal Code also penalizes defamation with a fine or up to one year in prison.⁵⁷

Meanwhile, several laws are designed to restrict and penalize legitimate online activities and speech. Most alarmingly, the 2012 Telecom Fraud Offences Law extends the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and criminal code to electronic communications sent over mobile phone and internet services.⁵⁸ The antiterrorism legislation prescribes prison sentences of up to 20 years for the publication of statements that can be understood as a direct or indirect encouragement of terrorism, which is vaguely defined.⁵⁹ The law also bans Voice over Internet Protocol (VoIP) services such as Skype⁶⁰ and requires all individuals to register their telecommunications equipment—including smartphones—with the government, which security officials typically enforce at security checkpoints by confiscating ICT equipment if the owner cannot produce a registration permit, according to sources in the country.

In June 2016, the Ethiopian government passed a new Computer Crime Proclamation that criminalized an array of online activities.⁶¹ For example, content that "incites fear, violence, chaos or conflict among people" can be punished with up to three years in prison, which could be abused to suppress digital

campaigns.⁶² Other problematic provisions ban the dissemination of defamatory content, which can be penalized with up to 10 years in prison,⁶³ and the distribution of unsolicited messages to multiple emails (spam), which carries up to five years in prison.⁶⁴ Civil society expressed concern that the law would be used to further crackdown on critical commentary, political opposition, and social unrest.⁶⁵

Prosecutions and Detentions for Online Activities

The authorities intensified their crackdown against bloggers, online journalists, and activists during the state of emergency in the past year. The antigovernment protest movement led to thousands of arrests, some for digital activities such as posting or “liking” social media content about the protests. Examples include the following:

In October 2016, police arrested Seyoum Teshome, a well-known academic and blogger for the Ethiopian Think Tank Group, who had published an article about the Oromia protest movement in *The New York Times*.⁶⁶ Teshome was held in prison for three months, during which he reported suffering severe torture (see *Intimidation and Violence*).⁶⁷

In November 2016, political activists Anania Sorri and Daniel Shibeshi and journalist Elias Gebru were arrested for posting images of themselves on social media displaying a gesture indicating support for the protest movement. Protest gestures and symbols were banned under emergency rule.⁶⁸

In December 2016, seven musicians behind a popular YouTube music video were arrested and held without charge until June 2017, when they were charged with terrorism. The video was held to incite protests.⁶⁹

Two cases led to convictions and multi-year prison sentences during the coverage period:

In May 2017, the prominent opposition activist Yonatan Tesfaye, was found guilty of terrorism based on Facebook posts that criticized the government’s handling of the Oromia protests.⁷⁰ He was sentenced to six and a half years in prison.⁷¹ Tesfaye’s Twitter handle has been active since his detention, leading to suspicions that the officials were using his account to monitor other dissidents or encourage them to break the law.⁷²

Also in May, Getachew Shiferaw, the editor-in-chief of the opposition outlet *Negere Ethiopia*, was sentenced to one and a half years in prison on subversion charges for Facebook comments were considered to “endorse” an exiled journalist.⁷³ He was released on time served.

Bloggers from the critical Zone 9 blogging collective were repeatedly persecuted during the coverage period, continuing several years of unabated legal troubles and harassment. The bloggers were first arrested in April 2014 and charged with terrorism under the harsh Anti-Terrorism Proclamation.⁷⁴ They were accused of intent to overthrow the government, an offense under the criminal code, by encrypting their communications to disseminate seditious writings.⁷⁵ Denied bail and brought to court dozens of times for sham trials,⁷⁶ the bloggers were eventually acquitted in late 2015, but the prosecutor appealed to the Supreme Court, and they were repeatedly summoned to appear throughout 2016.⁷⁷ In April 2017, the Supreme Court ruled that two of the Zone9 bloggers, Atnaf Berhane and Natnail Feleke, should be tried on charges of inciting violence through their writing. If convicted, they would face up to 10 years each in prison.⁷⁸

Other citizens were serving long prison sentences during the coverage period, including blogger Zelalem Workagenehu, who was found guilty of terrorism and sentenced to over five years in prison in May 2016.⁷⁹ He was first arrested in July 2014 on charges of conspiring to overthrow the government after he facilitated a course on digital security. Well-known dissident journalist and blogger Eskinder Nega is serving an 18-year prison sentence handed down in July 2012 under the draconian anti-terrorism law for criticizing the law itself in an online article.⁸⁰

Surveillance, Privacy, and Anonymity

Government surveillance of online and mobile phone communications is pervasive in Ethiopia and was strengthened under the new Computer Crime Proclamation enacted in June 2016, which enables real-time monitoring or interception of communications authorized by the Minister of Justice and obliges service providers to store records of all communications and metadata for at least a year.⁸¹

There are strong indications that the government has deployed a centralized monitoring system developed by the Chinese telecommunications firm ZTE to monitor mobile phone networks and the internet, according to a 2015 Human Rights Watch report.⁸² Known for its use by repressive regimes in Libya and Iran, the monitoring system enables deep packet inspection (DPI) of internet traffic across the EthioTelecom network and has the ability to intercept emails and web chats.

A customer management database called ZSmart, also developed by ZTE, has been installed by EthioTelecom. The database provides the government with full access to user information and the ability to intercept SMS text messages and record phone conversations.⁸³ ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.⁸⁴ While the extent to which the government has made use of the full range of ZTE's sophisticated surveillance systems is unclear, the authorities frequently present intercepted emails and phone calls as evidence during trials against journalists and bloggers or during interrogations as a scare tactic.⁸⁵

Meanwhile, exiled dissidents have been targeted by surveillance malware. Citizen Lab research published in March 2015 said Remote Control System (RCS) spyware had been used against two employees of Ethiopian Satellite Television Service (ESAT) in November and December 2014. ESAT is a diaspora-run independent satellite television, radio, and online news media outlet, based in Alexandria, Virginia.⁸⁶ Made by the Italian company Hacking Team, RCS spyware is advertised as "offensive technology" sold exclusively to law enforcement and intelligence agencies, and has the ability to steal files and passwords and intercept Skype calls and chats. ⁸⁷

While Hacking Team has said that the company does not deal with "repressive regimes,"⁸⁸ the social engineering tactics used to bait the two ESAT employees made it clear that the attack was targeted. Moreover, analysis of the RCS attacks uncovered credible links to the Ethiopian government, with the spyware's servers registered at an EthioTelecom address under the name "INSA-PC," referring to the Information Network Security Agency (INSA), the body established in 2011 to preside over the security of the country's critical communications infrastructure.⁸⁹ INSA was already known to be using the commercial toolkit FinFisher to target dissidents and supposed national security threats. FinFisher can secretly monitor computers by turning on webcams, record everything a user types with a key logger, and intercept Skype calls.⁹⁰

Political commentators use VPNs and anonymizing tools to hide their identities when publishing online and to circumvent filtering, though the tools are also subject to blocking (see Blocking and Filtering).

Anonymity is further compromised by strict SIM card registration requirements. Upon purchase of a SIM card through EthioTelecom or an authorized reseller, individuals must provide their full name, address, government-issued identification number, and a passport photograph. EthioTelecom's database of SIM registrants enables the government to terminate SIM cards and bar individuals from registering for new ones. Internet subscribers are also required to register their personal details, including their home address, with the government. During the antigovernment protests in 2016, state-owned ICT provider EthioTelecom announced plans to require mobile phones to be purchased from Ethiopian companies and to create a tracking system for all mobile devices in Ethiopia. Though no updates on the plans were reported in 2017, observers believe the plan aims to allow the government to track and identify all communications from subscribers on its network.⁹¹

Intimidation and Violence

During escalating antigovernment protests throughout 2016, the authorities routinely harassed, detained, and abused people who used their mobile phones to record footage of demonstrations. Under emergency rule, the authorities reportedly arrested thousands of people, some for their online activities. Imprisoned bloggers reported being held in degrading conditions and tortured by prison guards seeking to extract false confessions.⁹² In one case, blogger Seyoum Teshome, who was arrested after the publication of his critical New York Times op-ed, reported suffering severe torture while in detention from October to December 2016.⁹³

Government security agents frequently harass and intimidate bloggers, online journalists, and internet users. Independent bloggers are often summoned by the authorities to be warned against discussing certain topics online, while activists report that they are regularly threatened by state security agents.⁹⁴ Ethiopian journalists in the diaspora have also been targeted for harassment.⁹⁵

Technical Attacks

There were no reports of technical attacks against human rights defenders or dissidents during the coverage period, though incidents are likely underreported. Opposition critics have faced frequent technical attacks in the past, even abroad. Observers believe similar campaigns against activists persist undetected. Independent research has shown that Ethiopian authorities use sophisticated surveillance spyware to target exiled dissidents.⁹⁶

Notes:

1 Human Rights Watch, "Legal Analysis of Ethiopia's State of Emergency," October 30, 2016, <https://www.hrw.org/news/2016/10/30/legal-analysis-ethiopias-state-emergency>

2 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," <http://bit.ly/1cblxxY>

3 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2016," <http://bit.ly/1cblxxY>

4 Endalk Chala, "When blogging is held hostage of Ethiopia's telecom policy," in "GV Advocacy Awards Essays on Internet Censorship from Iran, Venezuela, Ethiopia," Global Voices (blog), February 3, 2015, <http://bit.ly/1OpDvzz>

5 Ethiopia – Telecoms, Mobile, Broadband and Forecasts, Paul Budde Communication Pty Ltd.: June 2014, <http://bit.ly/1ji15Rn>

6 William Davison's Facebook post, March 26, 2016, <https://www.facebook.com/william.davison.33/posts/10153956834545792?pnref=story>

7 http://a4ai.org/affordability-report/data/?_year=2017&indicator=INDEX&country=ETH

8 Jacob Poushter, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," Pew Research Center, February 22, 2016, <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>

9 According to tests by Freedom House consultant in 2016.

10 Endalk Chala, "Ethiopia Locks Down Digital Communications in Wake of #OromoProtests," Global Voices (blog), July 14, 2016, <https://globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests>; Moses Karanja et al., "Ethiopia: Internet Shutdown Amidst Recent Protests?" OONI, August 10, 2016, <https://ooni.torproject.org/post/ethiopia-internet-shutdown-amidst-recent-protests/> https://www.washingtonpost.com/world/africa/a-year-after-obamas-visit-ethiopia-is-in-turmoil/2016/08/09/d7390290-5e39-11e6-8e45-477372e89d78_story.html?utm_term=.03daaa5f6f70

11 Stephanie Busari, "Ethiopia declares state of emergency after months of protests," CNN, October 11, 2016, <http://www.cnn.com/2016/10/09/africa/ethiopia-oromo-state-emergency/>; Endalk Chala, "Ethiopian authorities shut down mobile internet and major social media sites," Global Voices (blog), October 11, 2016, <https://globalvoices.org/2016/10/11/ethiopian-authorities-shut-down-mobile-internet-and-major-social-media-sites/>

12 "Ethiopia: Third Internet shutdown follows imprisonment of two human rights activists," Article 19, June 7, 2017, <https://www.ifex.org/ethiopia/2017/06/06/internet-shutdown/>

13 Paul Schemm, "Ethiopia shuts down social media to keep from 'distracting' students," Washington Post, July 13, 2016, <https://www.washingtonpost.com/news/worldviews/wp/2016/07/13/ethiopia-shuts-down-social-media-to-keep-from-distracting-students/>; <http://www.newsweek.com/ethiopia-internet-blocked-618806>

14 Darrell M. West, "Internet shutdowns cost countries \$2.4 billion last year," Brookings Institute, Center for Technology Innovation, October 2016, <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>

15 "Economic Impact of Internet Disruptions in Sub-Saharan Africa," CIPESA, September 2017, <https://cipesa.org/2017/09/economic-impact-of-internet-disruptions-in-sub-saharan-africa/>

16 "Ethio Telecom to remain monopoly for now," TeleGeography, June 28, 2013, <http://bit.ly/1huyjf7>

17 Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," Telecentre Magazine, September 2008, <http://bit.ly/1ji348h>.

18 Paul Chapman, "New report explores the Ethiopian – telecoms, mobile and broadband – market insights, statistics and forecasts," WhatTech, May 1, 2015, <http://bit.ly/1L46Awu>.

19 "Out of reach," The Economist, August 24, 2013, <http://econ.st/1l1UvJO>.

20 "Out of reach," The Economist.

21 Matthew Dalton, "Telecom Deal by China's ZTE, Huawei in Ethiopia Faces Criticism," The Wall Street Journal, January 6, 2014, <http://on.wsj.com/1LtSCkD>.

22 Based on allegations that the Chinese authorities have provided the Ethiopian government with technology that can be used for political repression—such as surveillance cameras and satellite jamming equipment—in the past. See: Addis Neger, "Ethiopia: China Involved in ESAT Jamming," ECADAF Ethiopian news & Opinion, June 23, 2010, <http://bit.ly/1LtSYI9>; Gary Sands, "Ethiopia's Broadband Network – A Chinese Trojan Horse?" Foreign Policy Blogs, Foreign Policy Association, September 6, 2013, <http://bit.ly/1FWG8X1>.

23 ENA, "Ericsson to take part in telecom expansion in Ethiopia," Dire Tube, December 18, 2014, <http://bit.ly/1PkZfvA>.

24 The Embassy of the United States, "Doing Business in Ethiopia," <http://1.usa.gov/1LtTEh>.

25 World Intellectual Property Organization, "Ethiopia Custom Regulation: No 622/2009," <http://bit.ly/1NveoeB>.

26 Mignote Kassa, "Why Ethiopia's Software Industry Falters," Addis Fortune 14, no. 700 (September 29, 2013), <http://bit.ly/1VJiIWC>.

27 "Proclamation No. 281/2002, Telecommunications (Amendment Proclamation," Federal Negarit Gazeta No. 28, July 2, 2002, <http://bit.ly/1snLgsc>.

28 Ethiopian Telecommunication Agency, "License Directive for Resale and Telecenter in Telecommunication Services No. 1/2002," November 8, 2002, accessed October 20, 2014, <http://bit.ly/1pUtpWh>.

29 Dr. Lishan Adam, "Understanding what is happening in ICT in Ethiopia," (policy paper, Research ICT Africa, 2012) <http://bit.ly/1LDPyJ5>.

30 Halefom Abraha, "THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA," (paper) <http://bit.ly/1huzPOS>.

31 Rebecca Wanjiku, "Study: Ethiopia only sub-Saharan Africa nation to filter net," IDG News Service, October 8, 2009, <http://bit.ly/1Lbi3s9>.

32 Test conducted by an anonymous researcher contracted by Freedom House, March 2016. During the test, some websites opened at the first attempt but were inaccessible when refreshed.

33 Maria Xynou et al., "Ethiopia: Evidence of social media blocking and internet censorship," OONI, December 14, 2016, <https://ooni.torproject.org/post/ethiopia-report/>

34 Felix Horne, "Deafening silence from Ethiopia," Foreign Policy in Focus, April 12, 2016, <http://fpif.org/deafening-silence-ethiopia/>; Endalk Chala, "Ethiopia locks down digital communications in wake of #OromoProtests," Global Voices (blog), July 14, 2016, <https://advox.globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests/>; <https://phys.org/news/2017-06-internet-social-media-ethiopia-block.html>

35 Nicole Orttung, "Why did Ethiopia block social media," Christian Science Monitor, July 12, 2016, <http://www.csmonitor.com/World/2016/0712/Why-did-Ethiopia-block-social-media?cmpid=gigya-tw>

36 According to activists who were able to circumvent the blocks and observe the social media activities of progovernment users.

37 Ismail Akwei, "Ethiopia blocks social media to prevent university exam leakage," Africa News, July 10, 2016, <http://www.africanews.com/2016/07/10/ethiopia-blocks-social-media-to-prevent-university-exam-leakage/>

38 Endalk Chala, "Defending against overreaching surveillance in Ethiopia: Surveillance Self-Defense now available in Amharic," Electronic Frontier Foundation, October 1, 2015, <https://www.eff.org/deeplinks/2015/09/defending-against-overreaching-surveillance-ethiopia-surveillance-self-defense-n-0>

39 A 2014 report from Human Rights Watch also noted that the term "aljazeera" was unsearchable on Google while the news site was blocked from August 2012 to mid-March 2013. According to HRW research, the keywords "OLF" and "ONLF" (acronyms of Ethiopian opposition groups) are not searchable on the unencrypted version of Google (<http://>) and other popular search engines. Human Rights Watch, "They Know Everything We Do," March 25, 2014, 56, 58, <http://bit.ly/1Nviu6r>.

40 "Tor and Orbot not working in Ethiopia," Tor Stack Exchange, message board, April 12, 2016, <http://tor.stackexchange.com/questions/10148/tor-and-orbot-not-working-in-ethiopia>; "Ethiopia Introduces Deep Packet Inspection," Tor (blog), May 31, 2012, <http://bit.ly/1A0YRdc>; Warwick Ashford, "Ethiopian government blocks Tor network online anonymity," Computer Weekly, June 28, 2012, <http://bit.ly/1LDQ5L2>.

41 Daniel Berhane, "Ethiopia's web filtering: advanced technology, hypocritical criticisms, bleeding constitution," Horns Affairs, January 16, 2011, <http://bit.ly/1jTyrH1>

42 Kevin Mwanza, "Is Ethiopia restricting access to social media in Oromia region?" Afk Insider, April 13, 2016, <http://afkinsider.com/123180/ethiopia-restricting-access-social-media-oromia-region/>

43 Markos Lemma, "Disconnected Ethiopian Netizens," Digital Development Debates (blog), November 2012, <http://bit.ly/1MI9Nu3>.

44 Exemptions are made for foreign nationals of Ethiopian origin. See, Abrham Yohannes, "Advertisement Proclamation No. 759/2012," Ethiopian Legal Brief (blog), September 27, 2012, <http://bit.ly/1LDQf5c>.

45 "Proclamation No. 686/2010 Commercial Registration and Business Licensing," Federal Negarit Gazeta, July 24, 2010, <http://bit.ly/1P3PoLy>; World Bank Group, Doing Business 2015: Going Beyond Efficiency, Economy Profile 2015, Ethiopia, 2014, <http://bit.ly/1L49tO6>.

46 Chala, "When blogging is held hostage of Ethiopia's telecom policy."

47 "Ethiopia Trains Bloggers to attack its opposition," ECADF Ethiopian News & Opinions, June 7, 2014, <http://bit.ly/1QemZjl>.

48 The term "Koka" is a blend of two words: Kotatam and cadre. Kotatam is a contemptuous Amharic word used to imply that someone is a sellout who does not have a respect for himself or herself.

49 Endalk Chala, "Ethiopia protest videos show state brutality, despite tech barriers," Global Voices (blog), January 6, 2016, <https://advox.globalvoices.org/2016/01/06/ethiopia-protest-videos-show-state-brutality-despite-tech-barriers/>

50 Jacey Fortin, "The ugly side of Ethiopia's economic boom," Foreign Policy, March 23, 2016, <http://foreignpolicy.com/2016/03/23/no-one-feels-like-they-have-any-right-to-speak-at-all-ethiopia-oromo-protests/>

51 "Seven things banned under Ethiopia's state of emergency," BBC News, October 17, 2016, <http://www.bbc.com/news/world-africa-37679165>

52 "Social media blackout in Ethiopia," Jacarandafm, October 17, 2016, <https://www.jacarandafm.com/news-sport/news/social-media-blackout-in-ethiopia/>

53 "Ethiopia lifts state of emergency imposed in October," Associated Press, August 4, 2017, <http://www.startribune.com/ethiopia-lifts-state-of-emergency-imposed-in-october/438488273/>

54 Constitution of the Federal Democratic Republic of Ethiopia (1995), art. 26 and 29, accessed, August 24, 2010, <http://www.ethiobar.net/constitution>.

55 Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, Federal Negarit Gazeta No. 64, December 4, 2008.

56 Article 19, The Legal Framework for Freedom of Expression in Ethiopia, accessed September 10, 2014, <http://bit.ly/1PI0f33>.

57 Criminal Code, art. 613, <http://bit.ly/1OpHE6F>.

58 Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences," legal analysis, August 6, 2012, <http://bit.ly/1Lbonjm>.

59 “Anti-Terrorism Proclamation No. 652/2009,” Federal Negarit Gazeta No. 57, August 28, 2009.

60 The government first instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communication and began draining revenue from the traditional telephone business belonging to the state-owned EthioTelecom. In response to widespread criticisms, the government claimed that VoIP applications such as Skype would not be considered under the new law, though the proclamation’s language still enables the authorities to interpret it broadly at whim.

61 “Ethiopia Computer Crime Proclamation Text Draft,” Addis Insight, May 9, 2016, <http://www.addisinsight.com/2016/05/09/ethiopia-computer-crime-proclamation-text-draft/>

62 Article 14, “Crimes against Public Security,” Computer Crime Proclamation, draft text at <http://www.addisinsight.com/2016/05/09/ethiopia-computer-crime-proclamation-text-draft/>, <http://hornaffairs.com/en/2016/05/09/ethiopia-computer-crime-proclamation/>

63 Article 13, “Crimes against Liberty and Reputation of Persons,” Computer Crime Proclamation.

64 Article 15, “Dissemination of Spam,” Computer Crime Proclamation,

65 Kimberly Carlson, “Ethiopia’s new Cybercrime Law allows for more efficient and systematic prosecution of online speech,” Electronic Frontier Foundation, June 9, 2016, <https://www.eff.org/deeplinks/2016/06/ethiopias-new-cybercrime-law-allows-more-efficient-and-systematic-prosecution-online>; Tinishu Soloman, “New Ethiopian law targets online crime,” The Africa Report, June 9, 2016, <http://www.theafricareport.com/East-Horn-Africa/new-ethiopian-law-targets-online-crime.html>

66 “Oromo protests: Ethiopia arrests blogger Seyoum Teshome,” Al Jazeera, October 5, 2016, <http://www.aljazeera.com/news/2016/10/oromo-protests-ethiopia-arrests-blogger-seyoum-teshome-161005071925586.html>

67 “Seyoum Teshome released,” Frontline Defenders, accessed October 30, 2017, <https://www.frontlinedefenders.org/en/case/seyoum-teshome-released>

68 https://www.diretube.com/anania-sorri-elias-gebru-and-daniel-shibeshi-arrested-today-dw-amharic_7e64f070f.html; See also: Anania Sorri Facebook post, October 28, 2016, <http://bit.ly/2gwZTfQ>

69 <https://advox.globalvoices.org/2017/07/14/ethiopian-musicians-charged-with-terrorism-for-inciting-song-lyrics/>

70 Salem Soloman, “Ethiopia’s Anti-terrorism Law: Security or Silencing Dissent?” VOA News, May 31, 2016, <http://www.voanews.com/a/ethiopia-anti-terrorism-law-security-silencing-dissent/3356633.html>

71 “Ethiopia jails opposition politician Yonatan Tesfaye,” Al Jazeera, May 26, 2017, <http://www.aljazeera.com/news/2017/05/ethiopian-court-jails-politician-6-years-170525141848655.html>

72 @befeqadu Twitter post, April 12, 2016, <https://twitter.com/befeqadu/status/719963259911188480/photo/1>

73 “News: Ethiopia editor-in-chief sentenced for a year and half in prison, time he already served,” Addis Standard, May 26, 2017 “<http://addisstandard.com/news-ethiopia-editor-in-chief-sentenced-for-a-year-and-half-in-prison-time-he-already-served/>

74 “Six members of Zone Nine, group of bloggers and activists are arrested,” [in Amharic] Zone9 (blog), April 25, 2014, <http://bit.ly/1VJn6ow>; “Federal High Court Lideta Criminal Bench court, Addis Ababa,” <http://1drv.ms/1OqAjlC>.

75 Endalk Chala, “What You Need to Know About Ethiopia v. Zone9 Bloggers: Verdict Expected July 20,” Global Voices (blog), July 17, 2015, <http://bit.ly/1jTDO9b>.

76 Ellery Roberts Biddle, Endalk Chala, Guardian Africa network, “One year on, jailed Ethiopian bloggers are still awaiting trial,” The Guardian, April 24, 2015, <http://gu.com/p/47ktv/stw>; “Nine Journalists and Bloggers Still Held Arbitrarily,” Reporters Without Borders, “Nine Journalists and Bloggers Still Held Arbitrarily,” August 21, 2014, <http://bit.ly/1P3TW4l>.

77 “Netizen Report: Ethiopia’s Zone9 Bloggers Go Back to Court,” Global Voices (blog), March 30, 2016, <https://advox.globalvoices.org/2016/03/30/netizen-report-ethiopias-zone9-bloggers-go-back-to-court/>

78 “Ethiopia Supreme Court says two Zone 9 bloggers should face incitement charges,” CPJ, April 6, 2017, <https://cpj.org/2017/04/ethiopia-supreme-court-says-two-zone-9-bloggers-sh.php>

79 Tedla D. Tekle, “Ethiopian blogger and activist sentences to five years and four months,” Global Voices (blog), May 16, 2016, <https://advox.globalvoices.org/2016/05/16/ethiopian-blogger-and-activist-sentenced-to-five-years-and-four-months/>

80 Such trumped-up charges were based on an online column Nega had published criticizing the government’s use of the Anti-Terrorism Proclamation to silence political dissent and calling for greater political freedom in Ethiopia. Nega is also the 2011 recipient of the PEN/Barbara Goldsmith Freedom to Write Award. “That Bravest and Most Admirable of Writers: PEN Salutes Eskinder Nega,” PEN American Center (blog), April 13, 2012, <http://bit.ly/1Lm89Y7>; See also, Markos Lemma, “Ethiopia: Online Reactions to Prison Sentence for Dissident Blogger,” Global Voices, July 15, 2012, <http://bit.ly/1OpKaKf>; EndalkChala, “Ethiopia: Freedom of Expression in Jeopardy,” Global Voices Advocacy, February 3, 2012, <http://bit.ly/1jflEO3>.

81 Article 23, “Retention of Computer Data” and Article 24, “Real-time Collection of Computer Data,” <http://hornaffairs.com/en/2016/05/09/ethiopia-computer-crime-proclamation/>

82 Human Rights Watch, “They Know Everything We Do,” 62.

83 Human Rights Watch, “They Know Everything We Do,” 67.

84 Ibid, 52.

85 Committee to Protect Journalists, “Ethiopian Blogger, Journalists Convicted of Terrorism,” January 19, 2012, <http://cpj.org/x/47b9>.

86 Bill Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, Citizen Lab, March 9, 2015, <http://bit.ly/1Ryogmr>.

87 Hacking Team, “Customer Policy,” accessed February 13, 2014, <http://hackingteam.it/index.php/customer-policy>.

88 Declan McCullagh, “Meet the ‘Corporate Enemies of the Internet’ for 2013,” CNET, March 11, 2013, accessed February 13, 2014, <http://cnet.co/1fo6jJZ>.

89 Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.

90 Fahmida Y. Rashid, “FinFisher ‘Lawful Interception’ Spyware Found in Ten Countries, Including the U.S.,” Security Week, August 8, 2012, <http://bit.ly/1WRPuap>.

91 Endalk Chala, “Ethiopia Locks Down Digital Communications in Wake of #OromoProtests.”

92 Tedla D. Tekle, “‘I was forced to drink my own urine,’: ‘Freedom’ for netizen after 647 days locked up, but not for all.”

93 Seyoum Teshome, “A license to torture,” Amnesty International, March 28, 2017, <https://www.amnesty.org/en/latest/campaigns/2017/03/a-license-to-torture/>

94 SIMEGNISH (LILY) MENGESHA, “CRAWLING TO DEATH OF EXPRESSION – RESTRICTED ONLINE MEDIA IN ETHIOPIA,” Center for International Media Assistance (blog), April 8, 2015, <http://bit.ly/1IbxFie>.

95 “ከንፋ አሰፋ በስላላ ከሆላንድ የተባረረው የጋዜጠኛውን አንገት እቆርጣለሁ አለ,” ECADAF Ethiopian News & Opinion, April 12, 2015, <http://ecadforum.com/Amharic/archives/14790/>.

96 Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, March 2015, <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/> .