Ethiopia

Not Free
28
100

A Obstacles to Access  3 25
B Limits on Content    12 35
C Violations of User Rights 13 40

Last Year's Score & Status
17 100 Not Free

Overview

Ethiopia experienced a significant improvement in internet freedom during the coverage period, in large part due to changes implemented by the administration of newly appointed prime minister Abiy Ahmed. In June 2018, the government lifted a state of emergency and unblocked more than 260 websites. The localized network shutdowns that occurred during the second half of 2018 were significantly less severe than the nationwide network shutdowns and social media blocking of previous years. Harassment and arrests of users were also less common than in the
past. However, some new concerns emerged as the government began drafting a law on hate speech.

Abiy was appointed in April 2018 following sustained antigovernment protests. Although he represents the incumbent Ethiopian People’s Revolutionary Democratic Front (EPRDF), which has ruled Ethiopia since 1991, he has pledged to reform the authoritarian state and rewrite its repressive electoral, terrorism, and media laws. Despite the promising changes to date, the country remains beset by political factionalism and intercommunal violence, abuses by security forces and violations of due process are still common, and many restrictive laws remain in force.

Key Developments

June 1, 2018 – May 31, 2019

- Local network shutdowns were imposed in August and September 2018 (see A3). However, these disruptions were less severe than the nationwide shutdowns of the past.

- On June 22, 2018, the government reported that it had unblocked 264 websites, including news sites known for their critical reporting (see B1).

- Online media diversity improved as new outlets appeared and some previously blocked diaspora-based media and opposition sites, such as Ethiopian Satellite Television (ESAT) and Oromia Media Network (OMN), returned to the market (see B7).

- In a positive step in June, Prime Minster Abiy ended a state of emergency that had been imposed in February to quell escalating antigovernment protests. The measure had included restrictions on certain online activities, banning the circulation of “any information that could cause disturbance or suspicion” (see C1).

- The government was drafting a hate speech law during the coverage period that would reportedly penalize the publication of false information and carry a
jail term and fines for individuals who disseminate hate speech (see C2).

- The Committee to Protect Journalists reported that 2018 was the first year since 2004 in which Ethiopian authorities did not imprison a journalist (see C3). Some reporters for online outlets were briefly detained or assaulted during the coverage period, but conditions were generally less repressive than in the past (see C7).

A Obstacles to Access

Internet access expanded slightly but remained poor during the coverage period. While local network shutdowns were reported, this represented an improvement from past years, in which the government frequently instituted nationwide shutdowns and social media blocking. Efforts to privatize the state-owned telecommunications monopoly Ethio Telecom and open the information and communication technology (ICT) market to competition were under way.

A1 0-6 pts

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

Despite marginal gains in access, Ethiopia remains one of the least connected countries in the world, with an internet penetration rate of only 18.62 percent in 2017, compared with 15.36 percent in 2016, according to the latest data from the International Telecommunication Union. Although Ethio Telecom became the largest mobile provider in Africa in 2017, the reality in the country varies significantly from the official data regarding infrastructure and mobile penetration.

Public internet access is reportedly becoming more common. In major cities such as Addis Ababa, Bahir Dar, Mekele, Adama, Hawasa, and Dire Dawa, internet service and Wi-Fi are freely available in public places such as hotels, regional universities, phone shops, and internet cafés.

However, telecommunications infrastructure is almost entirely absent from rural areas, where more than 80 percent of the population resides. A handful of signal stations serve the entire country, resulting in network congestion and frequent
In smaller towns, users often hike to the top of the nearest hill to receive a stronger signal for their mobile devices.

The country has improved its internet speeds but still fares poorly in global rankings. In May 2019, Ethiopia was ranked 100 and 123 in Ookla’s SpeedTest global index for mobile data and fixed-line broadband, respectively. Ethiopia’s average mobile data download and upload speeds increased during the coverage period compared with a speed test conducted in Addis Ababa in May 2018, which found an average connection speed of 6.28 Mbps for downloading and 0.21 Mbps for uploading, with a 150-millisecond latency. Such slow speeds make it difficult to download even simple images. A test conducted by a Freedom House researcher in 2016 found that logging into an email account and opening a single message could take several minutes at a standard cybercafé with broadband in Addis Ababa, and even longer in rural areas. This finding remains largely unchanged.

- 3. https://www.wiman.me/ethiopia
- 6. https://www.speedtest.net/global-index/ethiopia#mobile

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?

The average advertised package for unlimited mobile internet service in Ethiopia costs 4,900 birr ($170) per month, which is prohibitively expensive for most Ethiopians. The price is kept artificially high due to state-owned Ethio Telecom’s monopoly. Ethiopians can spend an average of $100 per month for more limited mobile or fixed-line internet access. Better-quality services in neighboring Kenya
and Uganda cost less than $30 a month. In June 2018, Prime Minister Abiy’s government announced plans to privatize Ethio Telecom and open up the country’s telecommunications market to other players (see A4).4

In August 2018, Ethio Telecom introduced a new price package, stating that it had reduced rates by 43 percent for mobile internet service, 40 percent for voice calls, 43 percent for text messaging, and 54 percent for fixed-line broadband internet connections.5 Ethio Telecom now advertises a 25 MB data plan for 3 birr ($0.11) a day, a reduction from the 7 birr reported during the last coverage period. However, the 25 MB daily package is still extremely limited considering that a standard Google search uses up to 79 KB of data. Regularly loading websites containing 1 GB of multimedia content could cost $9 a day.6

Telecommunications devices, connection fees, and other related costs are also beyond the means of many Ethiopians. As a result, Ethiopia has among the lowest smartphone ownership rates in the world, at only 4 percent according to a 2016 Pew Research Center survey.7

Many Ethiopians rely on cybercafés, universities, and government offices for internet access. In rural areas and small towns, cybercafés are reportedly the most common means of accessing the internet. Cybercafé rates range from 7 to 10 birr ($0.25 to $0.35) for an hour of access. Rates in rural cybercafés tend to be higher. There have been some efforts to address the urban-rural divide and a gender gap in internet usage, such as Ethio Telecom’s plan to distribute free mobile phones to rural women.8 The impact of such efforts is unclear.

Digital literacy rates are generally low. Frequent power outages are common, even in the capital Addis Ababa, making internet service unreliable.

2. New reduced price for Ethiotelcom customers
   https://allafrica.com/stories/201811280630.html
   https://www.researchandmarkets.com/reports/4418557/ethiopia-telecoms-mo...
   https://www.wsj.com/articles/ethiopia-opens-door-to-the-world-with-unpr...
5. https://www.facebook.com/349142568566343/photos/a.349159025231364/11274...
A former Bloomberg’s Ethiopia correspondent, who was deported from Ethiopia in 2018, 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.” See: William Davison’s Facebook post, March 26, 2016, accessed September 21, 2018, https://www.facebook.com/william.davison.33/posts/10153956834545792?pnr...


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

Although the government interfered with internet access in Ethiopia during the coverage period, the disruptions were not as severe as in the past. The government has justified internet shutdowns, which sometimes occurred in the context of political rallies, by citing the need to maintain security and public order. In a positive change, most network connectivity in the country was restored after Prime Minister Abiy took office in April 2018, though localized shutdowns were reported in August and September 2018.

Fixed-line and mobile internet services were shut down from August 4 to August 26 in the eastern Somali region, where federal troops were engaged in clashes with local authorities. Mobile internet access was separately shut down from September 17 to September 19 in Addis Ababa following protests and an outbreak of ethnic violence. At least 23 people were killed in that unrest, with some estimates exceeding 50.

Until April 2018, internet and mobile phone service shutdowns were commonly imposed in response to large-scale demonstrations that began in late 2015—triggered by a government plan to appropriate land from the Oromia region for an expansion of the capital—and later spread to other regions and ethnic groups. For example, after student protests led to violent clashes in December 2017, the government imposed a blanket internet shutdown on all regional states, leaving
haphazard access available only in Addis Ababa. Mobile internet services were then shut down nationwide for several days following the resignation of Prime Minister Hailemariam Desalegn in February 2018, as the country was placed under a state of emergency. Oromia experienced another unexplained internet blackout for over two weeks in March 2018.

The process and legal underpinnings for shutdowns were not clear, though officials claimed that they were necessary to prevent ethnic violence and curb the spread of false news and hate speech. In second half of 2018 and the first half of 2019, it became less common for shutdowns to be linked to political rallies and public assemblies.

In June 2019, after the coverage period, one shutdown was imposed during national high school exams in a bid to prevent cheating, and another was implemented following an alleged coup attempt. Several social media platforms, including WhatsApp, Telegram, and Facebook, were blocked intermittently that month.

The Ethiopian government’s monopolistic control over the country’s telecommunications infrastructure via Ethio Telecom 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; instead it connects to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and another that passes through Djibouti to an international undersea cable. All connections to the international internet are completely centralized under Ethio Telecom, allowing the government to cut off traffic at will.

- 5. https://www.voanews.com/africa/23-killed-ethnic-violence-near-addis-aba...
A4 0-6 pts
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited, with Ethio Telecom holding a firm monopoly on internet and mobile phone services. In June 2018, Prime Minister Abiy’s government announced plans to privatize Ethio Telecom and open up the country’s market to other players. This process was still under way at the end of the coverage period. It had previously been reported in May 2018 that Ethio Telecom would subcontract a local private company to sell fixed-line internet services.

China is a key investor in Ethiopia’s telecommunications industry. Two major Chinese firms, ZTE and Huawei, were involved in upgrading Addis Ababa’s mobile broadband networks to fourth-generation (4G) technology and expanding 3G networks elsewhere. The partnership has enabled the Ethiopian state to maintain its hold over the telecoms sector, though the networks built by the Chinese firms have been criticized for their high cost and poor service. In May 2018, Beijing-based telecommunications company Hengbao was contracted to supply SIM cards for Ethio Telecom. These relationships have led to growing fears that Chinese entities may also be assisting the authorities in developing more robust ICT censorship and surveillance capacities (see C5).
Despite some movement toward reform, onerous government regulations are still in place and stymie other aspects of the Ethiopian ICT market. For example, 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. Ethiopians are required to register their laptops and tablet computers 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.

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

Cybercafés are subject to burdensome operating requirements under the Telecom Fraud Offences Proclamation of 2012, which prohibits them from providing Voice over Internet Protocol (VoIP) services and mandates that owners obtain a license from Ethio Telecom through an opaque process that can take months. Violations of the requirements entail criminal liability, though no cases have been reported.

6. Tang Shihua, “China’s Hengbao to Supply Ethiopia’s Telecom Monopoly With

“DOING BUSINESS IN ETHIOPIA,” THE EMBASSY OF THE UNITED STATES, ACCESSED SEPTEMBER 21, 2018, HTTPS://ET.USEMBASSY.GOV/BUSINESS/


BIRHANU FIKADE, “IT FIRMS ACCUSE INSA OF ‘CROWDING OUT,’” THE REPORTER, JUNE 17, 2017, HTTPS://WWW.THEREPORTEREHTIOPIA.COM/CONTENT/IT-FIRMS-ACCUSE-INSA-%E2%80%80...


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?

In February 2019 the government introduced a new proclamation establishing the...
Ethiopian Communications Regulatory Authority (ECRA) as the primary regulatory body overseeing the telecommunications sector. According to the draft proclamation, which was submitted to the parliament, the authority, which had yet to be established at the end of the coverage period,1 would have complete control over telecoms policy and sectoral regulation. ECRA will report to the prime minister, who will have some authority over the body, as he or she will appoint members to its board of directors and select its chair. In the past, the Ethiopian Telecommunications Agency was the primary regulatory body overseeing the telecommunications sector.2 The Information Network Security Agency (INSA), a government agency that has de facto authority over the internet with a mandate to protect the communications infrastructure and prevent cybercrime, has been placed under a new Ministry of Peace created by Abiy’s administration.

1. https://www.reuters.com/article/us-ethiopia-telecoms-exclusive/exclusive-
   https://addisstandard.com/wp-content/uploads/2019/02/Draft-Communicatio...

B Limits on Content

More than 260 websites were unblocked in June 2018, reflecting the new government’s increased openness to critical voices and independent news. Online media diversity improved as new outlets appeared and some previously blocked diaspora-based media and opposition sites returned to the market.

B1 0-6 pts

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

On June 22, 2018, the Ethiopian government reported that it had unblocked 264 websites, which was verified by the Open Observatory of Network Interference (OONI).1 The sites that became accessible included those of the US-based diaspora satellite television stations ESAT and OMN. Ayyantuu.net and Opride.com, prominent websites also known for their reporting on the country’s protests, became accessible as well.

With the exception of a few sites that were blocked during the most recent ethnic
violence, a manual test conducted in April 2019 by local researchers found that a large number of websites tested by Freedom House each year since 2012 remained unblocked, though several had not been updated for years and appeared abandoned. Three websites that were allegedly run by members of the previous government—Aiga Forum, Tigray Online, and Tigraisolidarity.org—were reportedly blocked in September 2018, but they were accessible during the test. The websites of international digital rights organizations, including the Electronic Frontier Foundation and Tactical Technology Collective, and select tools such as messaging applications and services on Google’s Android mobile operating system, which were inaccessible at irregular intervals during 2018, were all accessible during the 2019 test. Social media and communications platforms were available throughout the coverage period, except for those affected by the local network shutdowns in August and September 2018 (see A3).

Despite the recent improvements, Ethiopia still has a nationwide internet blocking and filtering system that can be redeployed at any time for political reasons. To filter the internet, specific internet protocol (IP) addresses or domain names are generally blocked at the level of the Ethio Telecom–controlled international gateway. Deep-packet inspection (DPI) is also employed, enabling blocking based on a keyword in the content of a website or of a communication such as an email message.

These capabilities were demonstrated in several cases after the coverage period. Facebook, WhatsApp, and Telegram were obstructed in June 2019, and the African Arguments website was apparently blocked as of early August.

In June 2019, when a Chicago-based LGBT+ tour company announced its plan to offer a trip to Ethiopia, it received online death threats, and its website was reportedly blocked temporarily in Ethiopia.
B2 0-4 pts
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

There were no reported cases of forced content removal by authorities during the coverage period, though nonstate actors such as organized youth groups began to coerce bloggers and other users to remove objectionable content, usually by way of threats. In the past, politically unfavorable content was often targeted for removal by security officials, who personally sought out users and bloggers and instructed them to take down the material in question.

B3 0-4 pts
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

There are no procedures for determining which websites are blocked or why, precluding any avenues for appeal. The authorities do not publish lists of blocked websites or criteria for how blocking decisions are made, and users receive a generic 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 INSA, Ethio Telecom, and the Ministry of Innovation and Technology—seem to maintain their own lists, contributing to a phenomenon of inconsistent blocking. The lack of transparency is exacerbated by the government’s typical refusal to admit its censorship efforts. Government officials have flatly denied the blocking of websites or jamming of international satellite operations while also stating that the government has a legal and a moral responsibility to protect the Ethiopian public from extremist content.
Do online journalists, commentators, and ordinary users practice self-censorship?

Media freedom and freedom of expression in Ethiopia were better respected during the coverage period than they had been in decades, but serious problems persist.

The government of Prime Minister Abiy eased state restrictions on the media, and citizens flocked to social media to participate in conversations about their country’s potential transition from authoritarianism and to hold the new government accountable for promised reforms. However, fear of reprisals by nonstate actors continued to encourage self-censorship (see C7). While most bloggers and journalists who were released from prison returned to their professional activity, they began to report concerns again in September 2018 and April 2019 as rising ethnic tensions led to violence and displacement.

Self-censorship remains common in the LGBT+ community. Same-sex sexual activity is a criminal offense in Ethiopia, deterring open discussion of related topics. Although there are various Ethiopian LGBT+ groups on Facebook, most are run by anonymous accounts.


Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?
Despite Ethiopia’s low levels of internet access, the former government was known to employ an army of online trolls to distort the information landscape.\(^1\) Opposition groups, journalists, and dissidents used the contemptuous Amharic colloquial term “Kokas” to describe the progovernment commentators.\(^2\) Observers say the Kokas regularly discussed Ethiopia’s economic growth in favorable terms and posted negative comments about Ethiopian journalists and opposition groups on Facebook and Twitter. In return, they were known to receive benefits such as money, land, and employment promotions.\(^3\) It is uncertain whether the new government has continued using the same online manipulation tactics, but supporters of the old government have accused the new government of doing so. They scornfully refer to supporters of the new regime as “Tekas.”

Some powerful nonstate actors also command large numbers of followers and trolls, especially on Facebook. There have been reports that online trolls pose as members of different ethnic groups to incite tensions between them.

Meanwhile, the spread of unconfirmed information, the phenomenon of false news, and the growing problem of hate speech in the context of ethnic clashes have had a major negative effect on the credibility of legitimate online information. For example, there was a flood of rumors on social media about the power struggle within the EPRDF coalition in the months before before the appointment of Abiy as prime minister in April 2018.


\(^2\) The term “Koka” is a blend of two words: Kotatam and cadre. Kotatam is used to imply that someone is a sellout who does not have respect for himself or herself.


B6 0-3 pts
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

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.”

The process for launching a website on the country’s .et domain is expensive and demanding, requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.


B7 0-4 pts

Does the online information landscape lack diversity?

Various constraints impede the development of diverse media outlets and perspectives online. The media environment often leans toward the government. While domestic usage of social media platforms, particularly Facebook, Twitter, and Instagram, has been expanding and slowly replacing the nascent Ethiopian blogosphere, the content often suffers from misinformation and polarization.
The media landscape has benefited from Prime Minister Abiy’s initial reforms. In addition to restored access for diaspora-based media and opposition outlets such as ESAT and OMN, a number of new online media outlets have appeared on the market.

Ethiopian online media lack diversity in some sensitive areas, such as coverage of LGBT+ issues.


B8 0-6 pts
Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues?

Despite hostile conditions caused by poor internet access and repressive laws, online activism has gained considerable momentum and influence over the past few years. Notably, social media and communications platforms have been integral to the mobilization of widespread antigovernment protests in the Oromia and Amhara regions since November 2015, enabling activists to post information about the demonstrations and disseminate news about police brutality as the government cracked down on protesters. Activists have also used social media platforms to consistently report on the arrests, trials, and releases of political prisoners.

In past coverage periods, the government routinely shut down networks and blocked social media in order to hinder mobilization efforts. While this did not take place on a large scale during the coverage period, the localized shutdowns in August and September 2018 were intended to disrupt public mobilization in the affected areas (see A3).

Since 2014 activists have employed social media to raise awareness about gender-based violence. In November 2018, activists created a hashtag and used Facebook for a 16-day campaign against such violence.

C Violations of User Rights

Prime Minister Abiy, who took office in April 2018, ended a state of emergency in June 2018, four months after it was imposed. A few bloggers were arrested for short periods during the state of emergency, but conditions for online freedom of expression subsequently improved.

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?

The law formally guarantees fundamental freedoms for Ethiopian internet users, but these rights have been routinely flouted in practice. The 1995 constitution provides for freedom of expression, freedom of the press, and access to information, while also prohibiting censorship. The 2008 Freedom of Mass Media and Access to Information Proclamation, known as the press law, affirms such constitutional safeguards. Nevertheless, the same law includes problematic provisions that restrict free expression, such as complex registration processes for media outlets and high fines for defamation. The criminal code penalizes defamation with a fine or up to one year in prison. These laws remained on the books under the new prime minister, though he promised to revise the press law. A new media bill was reportedly in draft form after the end of the coverage period.

To quell antigovernment protests that forced the resignation of Prime Minister Hailemariam Desalegn, the government imposed a six-month state of emergency in February 2018 that included restrictions on certain online activities, including a ban on the circulation of “any information that could cause disturbance or suspicion.” As with a previous state of emergency imposed from October 2016 to August 2017, the authorities also criminalized accessing or posting content related to the protests on social media, and any efforts to communicate with “terrorist” groups, a category that included exiled dissidents. Emergency rule undermined other fundamental rights, for example by prohibiting unauthorized protests and allowing security forces to arbitrarily arrest and detain citizens without charge. In a positive step,
Prime Minister Abiy, who took office in April 2018, ended the state of emergency in June, two months early. 7

5. https://www.hrw.org/news/2019/04/03/ethiopia-abiys-first-year-prime-min...

C2 0-4 pts
Are there laws that assign criminal penalties or civil liability for online activities?

Several laws designed to restrict and penalize legitimate online activities remain in place. The 2012 Telecom Fraud Offences Proclamation, for example, extends the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and the criminal code to electronic communications, including both mobile phone and internet services. 1 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 itself vaguely defined. 2 The law also bans VoIP services such as Skype, 3 and requires all individuals to register their telecommunications equipment—including smartphones—with the government. Security officials typically enforce that rule at checkpoints by confiscating ICT
equipment if the owner cannot produce a registration permit, according to sources in the country.

The 2016 Computer Crime Proclamation further criminalized an array of online activities. Civil society activists expressed concern that the law would be used to intensify a crackdown on critical commentary, political opposition, and public protest. For example, content that “incites fear, violence, chaos, or conflict among people” can be punished with up to three years in prison. Other problematic provisions ban the dissemination of defamatory content, which can be penalized with up to 10 years in prison, and the distribution of unsolicited messages to multiple email addresses (spam), which carries up to five years in prison.

More recently, officials including Prime Minister Abiy have started to express alarm about the potential for social media, particularly Facebook, to spread false news and exacerbate ongoing political tensions and ethnic violence. In November 2018 the government began drafting a hate speech law that could place restrictions on social media posts. The draft reportedly penalizes the publication of false information and imposes jail terms and fines for the dissemination of hate speech.

- 3. 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 criticism, 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 and at whim.
Are individuals penalized for online activities? 46

The Committee to Protect Journalists reported that 2018 was the first year since 2004 in which Ethiopian authorities did not imprison a journalist. In February 2019, Fasil Aragay of Mereja TV, an online news channel, and one of his colleagues were briefly detained by police—and then assaulted by a mob—while on duty in a suburb of Addis Ababa.1

After many years in which the authorities arrested antigovernment protesters and handed down long prison sentences to critical bloggers and journalists, the government stunned observers in January and February 2018 by releasing thousands of political prisoners, including blogger Eskinder Nega, who had been
serving an 18-year sentence since 2012. Bloggers who had been convicted on terrorism charges—Zelalem Workagegnehu, Yonatan Wolde, and Bahiru Degu, among others—were also eventually released, and outstanding charges against members of the critical Zone 9 blogging collective were dropped.

Despite these signs of progress, authorities made new arrests under the state of emergency imposed in February 2018. In March, police arrested Seyoum Teshome, a well-known academic and blogger, for criticizing the state of emergency online. He was released in April without charges. Separately, several bloggers and journalists were arrested on March 26 while at a social gathering, which were prohibited without prior authorization under the state of emergency. Those arrested included recently released Eskinger Nega, though they were all released after twelve days in prison.

Does the government place restrictions on anonymous communication or encryption?

Anonymous communication is 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-sized photograph. EthioTelecom’s database of SIM registrants enables the government to terminate individuals’ SIM cards and restrict them 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. Observers believe the plan aims to allow the government to track and identify all communications from subscribers on its network.¹

There are no explicit restrictions on encryption, though police officers or members of the security services may assume malign intent on the part of someone who uses encryption.


C5 0-6 pts

Does state surveillance of internet activities infringe on users’ right to privacy?

Government surveillance of online and mobile phone communications has been pervasive in Ethiopia, and the relevant laws and practices have not been reformed since the new prime minister took office in April 2018. During the coverage period, several activists reported that their phone communications were under surveillance.
The 2016 Computer Crime Proclamation strengthened the government’s surveillance powers, enabling real-time monitoring or interception of communications when authorized by the justice minister. The law also obliges service providers to store records of all communications and metadata for at least a year.1

Ethiopia’s telecommunications and surveillance infrastructure has been developed in part through investments from Chinese companies with backing from the Chinese government, creating strong suspicions that the Ethiopian government has implemented highly intrusive surveillance practices modeled on the Chinese system. These suspicions were reinforced in January 2018, when African Union officials accused China of hacking into its headquarters’ servers and secretly transferring data to servers in Shanghai over the course of five years, from 2012 to 2017.2 The state-owned China State Construction Engineering Corporation had built the African Union headquarters in Addis Ababa and connected the building’s telecommunications infrastructure through Ethio Telecom.

A 2015 Human Rights Watch report revealed strong indications that the Ethiopian government had deployed a centralized system developed by the Chinese telecommunications firm ZTE to monitor mobile phone networks and the internet.3 Known for its use by repressive regimes in Libya and Iran, the monitoring system facilitates DPI across the Ethio Telecom network and has the ability to intercept emails and web chats.

Another ZTE technology, known as ZSmart, is a customer management database installed at Ethio Telecom that provides the government with full access to user information and the ability to intercept SMS text messages and record phone conversations.4 ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.5 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 of journalists and bloggers, or as a scare tactic during interrogations.6

Meanwhile, exiled dissidents have been frequent targets of surveillance-enabling malicious software, or spyware, over the years. In February 2018, Citizen Lab published research detailing how spyware from an Israeli company had been used
against Jawar Mohammed, the exiled executive director of the diaspora-run news outlet OMN, which had been banned by the former Ethiopian government for allegedly inciting violence and promoting terrorism.7

Previous Citizen Lab research published in 2015 found that Remote Control System (RCS) spyware had been used against employees of ESAT, also a diaspora-run media outlet based in the United States, in 2014. RCS, a product of the Italian company Hacking Team, had been advertised as “offensive technology” sold to law enforcement and intelligence agencies around the world, with the ability to monitor user activity and steal data.8 While Hacking Team denied that it dealt with “repressive regimes,”9 analysis of the RCS attacks uncovered credible links to the Ethiopian government, with the spyware’s servers registered at an Ethio Telecom address under the name “INSA-PC,” an apparent reference to INSA, the government’s communications security agency.10

In a positive step, Prime Minister Abiy—who is regarded as one of the founders of INSA—forced the resignations of agency officials who were accused of monitoring and hacking activists, leading to some optimism that INSA may become less abusive regarding its surveillance powers.11

• 4. “They Know Everything We Do,” Human Rights Watch.
• 5. “They Know Everything We Do,” Human Rights Watch, page 52.
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

The Computer Crime Proclamation requires service providers to store records of all communications and related data for at least a year, and this information must be shared with the government if requested. 1

The lack of separation between state-owned Ethio Telecom and the government raises significant concerns about the company’s degree of cooperation with the government.


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

C6 0-6 pts

16

C7 0-5 pts

35
Harassment of and violence toward users still occur, though at lower levels than in the past. Prime Minister Abiy fired the head of Ethiopia’s prison service and other top officials in July 2018 based on allegations of systemic torture within the prison system.1

However, Dawit Wassihun Kassa, a journalist for the online news outlet Akiya Media, reported that he was assaulted in Ethiopia’s Southern Region in May 2019 while on assignment. He alleged that police officers were among those who assaulted and harassed him, and that the perpetrators accused him of spying.2

Also in May, activist Eskinder Nega, who has maintained a provocative presence on Twitter since his release from prison, received a threat from someone who pledged to physically attack him unless he ceased his online activities.3

Under the former government, security agents frequently harassed and intimidated bloggers, online journalists, and ordinary users. Independent bloggers were often summoned by the authorities, who warned them against discussing certain topics online, while activists reported that they were regularly threatened by state security agents.4 Ethiopian journalists in the diaspora were also targeted for harassment.5

Amid escalating antigovernment protests in 2017 and early 2018, the authorities reportedly harassed, detained, and abused several people who used their digital devices to record video of demonstrations. Political prisoners, many of whom were jailed for their online writings, have been subjected to grave human rights abuses, including torture, while in detention.6 Imprisoned bloggers reported being held in degrading conditions and tortured to extract false confessions.7

4. Simegnish (lily) Mengesha, “CRAWLING TO DEATH OF EXPRESSION – RESTRICTED ONLINE MEDIA IN ETHIOPIA,” Center for International Media Assistance, April 8, 2015, https://www.cima.ned.org/crawling-death-expression-restricted-online-me...
5. “,” ECADAF Ethiopian News & Opinion, Apr...

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

C8 0-3 pts

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

Daniel Berhane, an ardent supporter of the previous government who runs a news and opinion website, accused the new government of hacking his Facebook page in early 2019. According to local sources, his account was hacked, and some of his details were leaked. He subsequently regained control of the page.

Opposition critics and independent voices have faced frequent technical attacks over the years, even when based abroad. In February 2018, Citizen Lab published research detailing how spyware had been used to target Jawar Mohammed, the exiled executive director of OMN, throughout 2016 and 2017 (see C5).1


Country Facts

•
Freedom in the World Status

Not Free

- Networks Restricted
  Yes

- Social Media Blocked
  Yes

- Websites Blocked
  Yes

- Pro-government Commentators
  Yes

- Users Arrested
  No

Previous Reports

- 2018 Report