

Ethiopia

	2015	2016		
Internet Freedom Status	Not Free	Not Free	Population:	99.3 million
Obstacles to Access (0-25)	23	23	Internet Penetration 2015 (ITU):	12 percent
Limits on Content (0-35)	28	28	Social Media/ICT Apps Blocked:	Yes
Violations of User Rights (0-40)	31	32	Political/Social Content Blocked:	Yes
TOTAL* (0-100)	82	83	Bloggers/ICT Users Arrested:	Yes
			Press Freedom 2016 Status:	Not Free

* 0=most free, 100=least free

Key Developments: June 2015 – May 2016

- Internet and mobile phone networks were repeatedly disrupted around the country, particularly in the Oromia region during antigovernment protests that began in November 2015 (see **Restrictions on Connectivity**).
- Social media and communications platforms were temporarily blocked several times to restrict information about antigovernment protests and police brutality (see **Blocking and Filtering**).
- News websites were newly blocked for reporting on the Oromo protests and a severe drought, adding to a growing blacklist (see **Blocking and Filtering**).
- In May 2016, blogger Zelalem Workagenehu was sentenced to over five years in prison for leading a digital security course (see **Prosecutions and Arrests for Online Activities**).
- Prosecutors challenged the release of members of the Zone 9 blogging collective, after they were acquitted of terrorism charges in 2015 (see **Prosecutions and Arrests for Online Activities**).

Introduction

Internet freedom declined in the past year as the government cracked down on antigovernment protests and the digital tools citizens used to organize them.

Starting in the Oromo region in November 2015 as a protest against the authoritarian government's plan to infringe on land belonging to the marginalized Oromia people, the movement spread across the country in the subsequent months, turning into unprecedented demonstrations seeking regime change and democratic reform.

In a heavy-handed response, the authorities frequently shutdown local and national internet and mobile phone networks to prevent citizens from communicating about the protests. Social media platforms and communications apps such as Facebook, Twitter, Skype, and IMO were also temporarily blocked at different times. In October 2016, the government imposed a six-month state of emergency on October 17, resulting in another internet shutdown lasting several days. Under the state of emergency, accessing or posting content related to the protests on social media and efforts to communicate with "outside forces" are criminal offenses.

News websites and blogs reporting on the protests were permanently blocked in 2015 and 2016. Separately, critical news about the current drought—the worst the country has experienced in 50 years—was systematically censored. Meanwhile, the authorities arrested and prosecuted several bloggers, sentencing blogger Zelalem Workagenehu to five years in prison in May 2016. He was convicted of conspiring to overthrow the government for facilitating a course on digital security. The government's persecution of the Zone 9 bloggers continued. Though four of the bloggers were acquitted in October 2015, the prosecutor appealed their release to the Supreme Court, and they were repeatedly summoned throughout the year.

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 in many parts of the country throughout the year, particularly in the Oromia region during largescale antigovernment protests that erupted in November 2015. Meanwhile, poor infrastructure, obstructionist telecom policies, and a government monopoly on the 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 12 percent, according to 2015 data from the International Telecommunications Union (ITU).¹ Mobile

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," <http://bit.ly/1cblxY>

phone penetration is also poor at 43 percent, up from just 32 percent in 2014.² 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.³ 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.⁴ Price cuts announced in February 2016 mitigated some of the financial strain,⁵ bringing mobile internet prices to ETB 5 (US\$ 0.25) per day for 25 MB of data or ETB 3,000 (US\$ 140) per month for 30 GB. Nonetheless, the lower cost 25 MB package is extremely limited considering a standard Google search uses up to 79 KB alone. Regularly loading websites containing 1 GB of multimedia content could cost US\$ 9 a day. 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.

Telecommunication 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 recent Pew survey.⁷ In April 2016, EthioTelecom proposed a new pricing scheme to charge more for the use of popular Voice-over-IP (VoIP) platforms such as Viber and Facebook Messenger on mobile devices.⁸ This would make smartphone usage even more expensive.

Consequently, the majority of internet users still rely on cybercafés for internet access. A typical internet user in 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 cybercafés are higher. In addition, digital literacy rates are generally low.

For the few Ethiopians who can access the internet, connection speeds have been painstakingly slow for years, despite the rapid technological advances improving service quality in other countries. In a test conducted in the capital Addis Ababa,⁹ the average connection speed during one week

2 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2015," <http://bit.ly/1cblxxY>

3 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>

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

5 Misak Workneh, "Ethio Telecom announces new mobile internet packages, tariff revisions," *Addis Fortune*, February 23, 2016, <http://addisfortune.net/articles/ethio-telecom-announces-new-mobile-internet-packages-tariff-revisions/>

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

7 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/>

8 Eskedar Kifle, "Ethio telecom may charge for VoIP apps," *Capital Ethiopia*, April 6, 2016, <http://mereja.com/news/1149276>.

9 Test conducted by Freedom House researcher in March 2016. While the speed test should not be interpreted as a standard speed for the entire EthioTelecom network speeds, the data we gathered from a repeated speed tests over a span of a week from March 16 to March 21, 2016 suggest that Ethiopia's average speed lags behind the average speed of the region. Nearly same figures were reported by speed-test services such as <http://testmy.net> and <http://www.dospeedtest.com>.

in March 2016 was 1.2 Mbps—five times slower than the average 5.5 Mbps connection speed in Kenya. According to Akamai, the average connection speed in Ethiopia was 3 Mbps in the first quarter of 2016, significantly lower than the global average of 6.3 Mbps (Kenya's average speed was documented at 7.3 Mbps in the same period).¹⁰

In practice, such speeds result in extremely sluggish download times, even of simple images. Logging into an email account and opening a single message can take as long as five minutes at a standard cybercafé with broadband in the capital city, while attaching documents or images to an email can take eight minutes or more.¹¹ On mobile connections, Akamai found Ethiopia had the world's slowest average load time, at 8.5 seconds.¹²

Compounding Ethiopia's onerous access issues, severe drought in 2015 and 2016 has had a negative impact on the country's hydroelectric electricity production,¹³ resulting in frequent and extended power outages that limit users' ability to access the internet even further.¹⁴

Restrictions on Connectivity

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. In 2015–16, the flow of online traffic into, within, and out of Ethiopia registered a significant decline, likely as a result of network throttling, repeated internet shutdowns, and increased blocking.

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.

Internet and mobile phone networks were disrupted in many parts of the country throughout the year. Oromia, the largest of the federal republic's nine regional states, has experienced frequent telecom network since November 2015 saw the start of largescale demonstrations against the government's plan to appropriate Oromia territory.¹⁵ The protest movement escalated and remained ongoing in late 2016, leading the government to declare a six-month state of emergency and shut down mobile internet services nationwide for several days in October.¹⁶

10 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, <http://akamai.me/1LiS6KD>

11 According to tests by Freedom House consultant in 2016.

12 Akamai, "State of the Internet, Q1 2016 Report," <https://goo.gl/TQH7L7>.

13 William Davison, "Ethiopia Sees Nationwide Power Cuts While Drought Dries Dams," Bloomberg, December 1, 2015, <http://www.bloomberg.com/news/articles/2015-12-01/ethiopia-sees-nationwide-power-cuts-while-drought-dries-dams>

14 Mengisteab Teshome, "Ethiopia: Power Outage Taken as 'Business As Usual' – Residents," The Ethiopian Herald, September 4, 2015, <http://allafrica.com/stories/201509040955.html>

15 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/>

16 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/>

In an incident unrelated to the protests, internet services on computers and mobile devices were shut down for 24 hours in July 2016, ostensibly to prevent students from cheating during national university exams.¹⁷

The ICT shutdowns have been costly. Network disruptions between July 1, 2015 and June 30, 2016 cost Ethiopia's economy over US\$ 8.5 million, according to the Brookings Institution.¹⁸

ICT Market

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited,¹⁹ with state-owned EthioTelecom holding 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.²⁰

China is a key investor in Ethiopia's telecommunications industry,²¹ 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.²² The partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector,²³ though the networks built by the Chinese firms have been criticized for their high cost and poor service.²⁴ 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).²⁵ In December 2014, the Swedish telecom group Ericsson also partnered with the government to improve and repair the mobile network infrastructure,²⁶ 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.²⁷ Ethiopians are required register their laptops and tablets at the airport with the Ethiopian customs authority before they travel out of the country,

17 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/>

18 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>

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

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

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

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

23 "Out of reach," *The Economist*.

24 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>.

25 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/1LtSY19>; Gary Sands, "Ethiopia's Broadband Network – A Chinese Trojan Horse?" *Foreign Policy Blogs*, Foreign Policy Association, September 6, 2013, <http://bit.ly/1FWG8X1>.

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

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

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.²⁸

Local software companies also suffer from heavy-handed government regulations, which do not have fair, open, or transparent ways of evaluating and awarding bids for new software projects.²⁹ 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.

Cybercafés are subject to burdensome operating requirements under the 2002 Telecommunications (Amendment) Proclamation,³⁰ 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 cybercafés, reportedly penalizing Muslim cafe owners more harshly. Violations of the requirements entail criminal liability, though no cases have been reported.³¹

Regulatory Bodies

Since the emergence of the internet in Ethiopia, the Ethiopian Telecommunications Agency (ETA) has been the primary regulatory body overseeing the telecommunications sector. In practice, government executives have complete control over ICT policy and sector regulation.³² The Information Network Security Agency (INSA), a government agency established in 2011 and controlled by individuals with strong ties to the ruling regime,³³ also has significant power in regulating the internet under the mandate of protecting the communications infrastructure and preventing cybercrime.

Limits on Content

News websites known for their reporting on the Oromo protests joined Ethiopia's growing list of blocked content, while social media and communications platforms were blocked for periods of time throughout the coverage period for their role in disseminating information about the demonstrations and police brutality. The government manipulates online content, disseminating propaganda to convince Ethiopians that social media is a dangerous tool co-opted by opposition groups to spread hate and violence.

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

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

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

31 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>.

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

33 Halefom Abraha, "THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA," (paper) <http://bit.ly/1huzP0S>.

Blocking and Filtering

One of the first African countries to censor the internet,³⁴ Ethiopia has a nationwide, politically motivated internet blocking and filtering regime that is reinforced during sensitive political events. More websites were newly blocked during the Oromia protests that began in November 2015. Targets included the websites of US-based diaspora satellite television stations such as Ethiopian Satellite Television (ESAT) and the Oromo Media Network (OMN), which provided wall-to-wall coverage of the antigovernment protests. Ayyantuu.net and Opride.com, prominent websites also known for their reporting on the protests, were also blocked.³⁵

In an apparent attempt to restrict news about the protests from spreading, social media and file-sharing platforms such as Facebook, Twitter, WhatsApp, and Dropbox were repeatedly blocked for periods of time throughout the protests.³⁶ The blocks on social media first impacted networks in the Oromia region but later spread to other regions,³⁷ and eventually manifested in a shutdown of entire internet and mobile networks for days at a time (see Restrictions on Connectivity).

Unrelated to the protests, the authorities blocked access to social media and communications platforms, including Facebook, Twitter, Instagram, Viber, IMO, and Google+, to prevent cheating during university examinations on July 9 and 10, 2016.³⁸ The blocks followed a 24-hour 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,³⁹ which reinforced the belief that the government imposes restrictions on citizens while keeping the web open for its own advantage. Viber and IMO, two popular voice-over-IP applications, remained blocked until July 20, according to local sources.⁴⁰

Separately, coverage of a severe drought—the worst the country has experienced in 50 years—was systematically censored in the past year, with news websites and blogs blocked for reporting on the impact of the disaster that strayed from the government’s official narrative.⁴¹

In total, over one hundred websites are inaccessible in Ethiopia.⁴² A manual test conducted on the ground in mid-2016 confirmed that a large number of the websites tested by Freedom House each

34 Rebecca Wanjiku, “Study: Ethiopia only sub-Saharan Africa nation to filter net,” IDG News Service, October 8, 2009, <http://bit.ly/1Lbj3s9>.

35 “Ayyaantuu website blocked in Ethiopia,” Ayyaantuu News, March 3, 2016, <http://www.ayyaantuu.net/ayyaantuu-website-blocked-in-ethiopia/>

36 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://advoc.globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests/>

37 William Davison, “Twitter, WhatsApp Down in Ethiopia Oromia Area After Unrest,” Bloomberg, April 12, 2016, <http://www.bloomberg.com/news/articles/2016-04-12/twitter-whatsapp-offline-in-ethiopia-s-oromia-area-after-unrest>

38 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>

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

40 @befeqadu Twitter post, July 17, 2016, <https://twitter.com/befeqadu/status/754725025610104833>

41 Christabel Ligami, “Defying censorship, hunger stories emerge from Ethiopia,” Equal Times, April 29, 2016, <http://www.equaltimes.org/defying-censorship-hunger-stories?lang=en#.WBJZxMmFs6E>; “Ethiopian police detain journalists reporting on drought, escort them back to capital,” Committee to Protect Journalists, August 17, 2016, <https://cpj.org/2016/08/ethiopian-police-detain-journalists-reporting-on-d.php>

42 Test conducted by an anonymous researcher contracted by Freedom House, March 2015. During the test, some websites opened at the first attempt but were inaccessible when refreshed.

year since 2012 remained blocked. Blocked sites include Ethiopian news websites, political party websites, and the websites of international digital rights organizations, such as the Electronic Frontier Foundation and Tactical Technology Collective. Select tools such as text messaging apps and services on Google's Android operating system on smartphones were also inaccessible, but at irregular intervals and for unclear reasons.⁴³

Notably, several websites that hadn't been updated for years and appeared abandoned became accessible again in 2016, likely because the authorities deemed them no longer threatening. The social media curation tool Storify—first blocked in July 2012⁴⁴—was also newly accessible during the coverage period,⁴⁵ in addition to the URL shortening tool Bit.ly.⁴⁶

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) is also employed, which blocks websites based on a keyword in the content of a website or communication (such as email).⁴⁷

Digital security tools are also pervasively blocked in Ethiopia, including Tor, the circumvention tool that enables users to browse anonymously, which been blocked since May 2012.⁴⁸ As 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.⁴⁹ Local sources suspected progovernment commenters were flagging the same tools to be blocked by the authorities. The Amharic translation of the Electronic Frontier Foundations' "Surveillance Self-Defense" web guide was blocked two weeks after it was published in October 2015.⁵⁰ One source reported that key terms such as "proxy" yield no search results on unencrypted search engines,⁵¹ reflecting the government's efforts to limit users' access to circumvention tools and strategies.

Some restrictions are also placed on content transmitted via mobile phones. Text messages to more than ten recipients require prior approval from EthioTelecom.⁵² A bulk text message sent without prior approval is automatically blocked, irrespective of the content.

43 @AtnafB Twitter post, July 17, 2016, <https://twitter.com/AtnafB/status/754711725967024131>

44 Mohammed Ademo, Twitter post, July 25, 2012, 1:08 p.m., <https://twitter.com/OPride/status/228159700489879552>.

45 Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," *Columbia Journalism Review*, August 13, 2012, <http://bit.ly/1Lm2npk>.

46 Ory Okolloh Mwangi, Twitter post, November 6, 2013, 9:20 a.m., <https://twitter.com/kenyanpundit/status/398077421926514688>.

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

48 "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>.

49 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/>

50 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>

51 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>.

52 Interview with individuals working in the telecom sector, as well as a test conducted by a Freedom House consultant who found it was not possible for an ordinary user to send out a bulk text message.

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 government's continued denial of its censorship efforts. Government officials flatly deny 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.

Content Removal

Politically objectionable 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 being closely monitored. For instance, during the various legal proceedings involving the Zone 9 bloggers in 2015, friends and reporters who posted pictures and accounts of the trials on social media were briefly detained and asked to remove the posts.⁵³ During protests in Oromia, activists who wrote messages of solidarity for the protestors on Facebook were also asked to delete their posts.⁵⁴

Media, Diversity, and Content Manipulation

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."⁵⁵ The process for launching a website on the local .et domain is expensive and demanding,⁵⁶ requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.⁵⁷ While the domestic Ethiopian blogosphere has been expanding, most blogs are hosted on international platforms or published by members of the diaspora community.

Despite Ethiopia's extremely low levels of internet access, the government employs an army of trolls to distort Ethiopia's online information landscape.⁵⁸ Opposition groups, journalists, and dissidents use the contemptuous Amharic colloquial term, "Kokas," to describe the progovernment commentators.⁵⁹ Observers say the Kokas regularly discuss Ethiopia's economic growth in favorable

53 Reporters prevented from reporting on the trial of Zone9 Bloggers. See, Trial Tracker Blog, <http://trialtrackerblog.org/home/>.

54 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/>

55 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>.

56 "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>.

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

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

59 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.

terms and post uncomplimentary 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.⁶⁰ That characterization has been debunked by research. The University of Oxford and Addis Ababa University analyzed thousands of comments made by Ethiopians on Facebook during general election in 2015, finding that hate speech was a marginal proportion of the total comments assessed.⁶¹

Meanwhile, increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly in response to the spate of blogger arrests that have increased in the past few years (see Prosecutions and Detentions for Online Activities). Many bloggers publish anonymously to avoid reprisals.⁶² Fear of pervasive surveillance has also led to widespread self-censorship. Local newspapers and web outlets primarily publish reporting by regime critics and opposition organizations in the diaspora. Few independent local journalists will write for either domestic or overseas online outlets due to the threat of repercussions.

Digital Activism

Despite oppressive conditions caused by poor access and the hostile legal environment, online activism has gained considerable momentum and influence in the past year, particularly as traditional media coverage of current events has become increasingly narrow and dominated by pro-government voices. Notably, social media and communications platforms helped tech-savvy Ethiopians launch the widespread antigovernment protests in the Oromia region in November 2015. Online tools have been essential to the #OromoProtests movement, enabling activists to post information about the demonstrations and disseminate news about police brutality as the government cracked down on protesters.⁶³ The use of such tools to fuel the protest movement led the government to block access to several platforms throughout the year, and shut down internet and mobile networks altogether (see Blocking and Filtering and Restrictions on Connectivity).

Violations of User Rights

The new 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 or interception of communications. Several bloggers were arrested and prosecuted, with one blogger sentenced to five years in prison, while prosecutors challenged the acquittal of the Zone 9 bloggers.

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

61 Iginio Gagliardone et al., "Mechachal: Online debates and elections in Ethiopia. Report One: A preliminary assessment of online debates in Ethiopia," working paper, October 2, 2015, <http://bit.ly/2eOLFCH>

62 Markos Lemma, "Disconnected Ethiopian Netizens," Digital Development Debates (blog), November 2012, <http://bit.ly/1M19Nu3>.

63 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/>

Legal Environment

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.⁶⁴ 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.⁶⁵ 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 high fines for defamation.⁶⁶ The Criminal Code also penalizes defamation with a fine or up to one year in prison.⁶⁷

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, which explicitly include both mobile phone and internet services.⁶⁸ 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.⁶⁹ The law also bans Voice over Internet Protocol (VoIP) services such as Skype⁷⁰ 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.⁷¹ Civil society expressed concern that the law would be used to further crackdown on critical commentary, political opposition, and social unrest.⁷² 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.⁷³ Other problematic provisions ban the dissemination of defamatory content, which can be penalized with up to 10 years

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

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

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

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

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

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

70 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.

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

72 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 Solomon, “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>

73 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/>

in prison,⁷⁴ and the distribution of unsolicited messages to multiple emails (spam), which carries up to five years in prison.⁷⁵

To quell escalating antigovernment protests that began in the Oromia region in November 2015, the government imposed a six-month state of emergency on October 17, 2016 that included restrictions on certain online activities.⁷⁶ In addition to shutting down the internet for several days, the authorities criminalized the access and posting of content related to the protests on social media, as well as efforts to communicate with “terrorist” groups, a category that includes exiled dissidents. Penalties for violating the state of emergency include prison terms of three to five years.⁷⁷

Prosecutions and Detentions for Online Activities

In the past few years, the authorities have intensified their crackdown against bloggers and online journalists, using harsh laws to arrest and prosecute individuals for their online activities and silence dissent. The most high-profile prosecutions were against six bloggers from the critical Zone 9 blogging collective, who were arrested in April 2014,⁷⁸ and charged with terrorism under the harsh Anti-Terrorism Proclamation in July.⁷⁹ The bloggers were accused of intent to overthrow the government, an offense under the criminal code, by encrypting their communications to disseminate seditious writings.⁸⁰

Despite widespread international condemnation, the detainees were denied bail and brought to court dozens of times for over a year,⁸¹ until two of them were unexpectedly released without charge in early July 2015, immediately before U.S. President Obama visited Ethiopia. The four remaining Zone 9 bloggers were acquitted in October 2015,⁸² though they were barred from leaving the country.⁸³ The prosecutor contested their acquittal and appealed to the Supreme Court, and the four were summoned in December 2015 and in October 2016.⁸⁴ They were scheduled to return to court in November 2016.⁸⁵

Several other bloggers were arrested and prosecuted in the past year, including Getachew

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

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

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

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

78 “Six members of Zone Nine, group of bloggers and activists are arrested,” [in Amharic] Zone9 (blog), April 25, 2014, <http://bit.ly/1Vn6ow>.

79 “Federal High Court Lideta Criminal Bench court, Addis Ababa,” <http://1drv.ms/1OqAjlC>.

80 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>.

81 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/1P3TW4I>.

82 Committee to Protect Journalists, “In Ethiopia, Zone 9 bloggers acquitted of terrorism charges,” news statement, October 16, 2015, <https://www.cpj.org/2015/10/in-ethiopia-zone-9-bloggers-acquitted-of-terrorism.php>.

83 Gregory Warner, “Freed from prison, Ethiopian bloggers still can’t leave the country,” NPR, May 31, 2016, <http://www.npr.org/sections/parallels/2016/05/31/480100349/freed-from-prison-ethiopian-bloggers-still-cant-leave-the-country>

84 “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/>

85 “Netizen Report: As Protests Rage in Ethiopia, Zone9 Bloggers Return to Court,” Global Voices (blog), October 21, 2016, <https://globalvoices.org/2016/10/21/netizen-report-as-protests-rage-in-ethiopia-zone9-bloggers-return-to-court/>

Shiferaw, editor-in-chief of the online newspaper *Negere Ethiopia*, in December 2015.⁸⁶ *Negere Ethiopia* is known for its affiliation with the opposition as well as its coverage of the Zone 9 trials. Shiferaw remained in pretrial detention in mid-2016.⁸⁷

The prominent opposition member Yonatan Tesfaye was arrested in December 2015 and charged with terrorism based on Facebook posts that criticized the government's handling of the Oromia protests.⁸⁸ He remained in prison in mid-2016 and faces the death sentence if convicted.⁸⁹ Tesfaye's Twitter handle has been active during his detention, leading to suspicions that the officials have been using his account to bait potential dissidents.⁹⁰

In April 2016, blogger Zelalem Workagenehu was found guilty of terrorism and sentenced to over five years in prison in May.⁹¹ He was first arrested in July 2014 on charges of conspiring to overthrow the government after he facilitated a course on digital security. In the same trial, bloggers Yonatan Wolde and Bahiru Degu were acquitted after spending nearly two years in detention on terrorism charges; they were also arrested in July 2014 for applying to participate in Workagenehu's digital security course.⁹² Workagenehu has appealed to the Supreme Court.⁹³

The ongoing antigovernment protest movement has also led to numerous arrests, some for digital activities, including posting or "liking" social media content about the protests. In October 2016, police arrested Seyoum Teshome, a well-known academic and blogger for the Ethiothinktank.com website who had published an article about the Oromia protest movement in *The New York Times*.⁹⁴

Meanwhile, the 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.⁹⁵

Surveillance, Privacy, and Anonymity

Government surveillance of online and mobile phone communications is pervasive in Ethiopia

86 "Ethiopia arrests second journalist in a week, summons Zone9 bloggers," Committee to Protect Journalists, press release, December 27, 2015, <https://www.cpj.org/2015/12/ethiopia-arrests-second-journalist-in-a-week-summo.php>

87 "Getachew Shiferaw – The Price of Freedom of Expression in Ethiopia," Ethiopian Human Rights Project, May 3, 2016, <http://ehrp.org/getachew-shiferaw-the-price-of-freedom-of-expression-in-ethiopia/>

88 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>

89 "Ethiopia: Release opposition politician held for Facebook posts," Amnesty International, press release, May 6, 2016, <https://www.amnesty.org/en/latest/news/2016/05/ethiopia-release-opposition-politician-held-for-facebook-posts/>; "Facebook post leads to serious charges for Ethiopian politician," Enca, May 6, 2016, <http://bit.ly/2ewu9SU>

90 @befeqadu Twitter post, April 12, 2016, <https://twitter.com/befeqadu/status/71996325991188480/photo/1>

91 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/>

92 Tedla D. Tekle, "I was forced to drink my own urine; 'Freedom' for netizen after 647 days locked up, but not for all," Global Voices (blog), May 2, 2016, <http://bit.ly/2fxUWPs>

93 "Co-blogger Zelalem Workagenehu's appeal heard, appointed to tomorrow," De Birhan (blog), July 20, 2016, <http://debirhan.com/?p=10035>

94 "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>

95 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>; Endalk Chala, "Ethiopia: Freedom of Expression in Jeopardy," *Global Voices Advocacy*, February 3, 2012, <http://bit.ly/1jfiEO3>.

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.⁹⁶

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.⁹⁷ 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.

Another ZTE technology, known as ZSmart, is a customer management database installed at EthioTelecom that provides the government with full access to user information and the ability to intercept SMS text messages and record phone conversations.⁹⁸ ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.⁹⁹ 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.¹⁰⁰

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.¹⁰¹ Made by the Italian company Hacking Team, RCS spyware is advertised as "offensive technology" sold exclusively to law enforcement and intelligence agencies around the world, and has the ability to steal files and passwords and intercept Skype calls and chats.¹⁰²

While Hacking Team has said that the company does not deal with "repressive regimes,"¹⁰³ 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.¹⁰⁴ 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.¹⁰⁵

96 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/>

97 Human Rights Watch, "They Know Everything We Do," 62.

98 Human Rights Watch, "They Know Everything We Do," 67.

99 Ibid, 52.

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

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

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

103 Declan McCullagh, "Meet the 'Corporate Enemies of the Internet' for 2013," *CNET*, March 11, 2013, accessed February 13, 2014, <http://cnet.co/1fo6jJZ>.

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

105 Fahmida Y. Rashid, "FinFisher 'Lawful Interception' Spyware Found in Ten Countries, Including the U.S.," *Security Week*, August 8, 2012, <http://bit.ly/1WRPuap>.

Given the high degree of online repression in Ethiopia, political commentators use proxy servers 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-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.¹⁰⁶

While the government's stronghold over the Ethiopian ICT sector enables it to proactively monitor users, its access is less direct at cybercafés. For a period following the 2005 elections, cybercafé owners were required to keep a register of their clients, but the requirement has not been enforced since mid-2010.¹⁰⁷ Nevertheless, some cybercafé operators have reported that they are required to report "unusual behavior" to security officials, who also visit cybercafés (sometimes in plainclothes) to ask questions about individuals or monitor activity themselves.¹⁰⁸

Intimidation and Violence

Government security agents frequently harass and intimidate bloggers, online journalists, and ordinary users for their online activities. 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.¹⁰⁹ Ethiopian journalists in the diaspora have also been targeted for harassment.¹¹⁰

Amidst escalating antigovernment protests in 2015 and 2016, the authorities reportedly harassed, detained, and abused several people who used their mobile phones to record footage of demonstrations.

Meanwhile, imprisoned bloggers reported being held in degrading conditions and tortured by prison guards seeking to extract false confessions.¹¹¹ Yonatan Wolde and Bahiru Degu were re-arrested shortly after their acquittal in April 2016 and released the next day, reporting that officials had threatened their lives.¹¹²

106 Endalk Chala, "Ethiopia Locks Down Digital Communications in Wake of #OromoProtests."

107 Groum Abate, "Internet Cafes Start Registering Users," *The Capital* republished *Nazret* (blog), December 27, 2006, <http://bit.ly/1Lm98aX>.

108 Human Rights Watch, "They Know Everything We Do," 67.

109 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>.

110 "ከንፉ አለፋ በስለ ከሆላንድ የተባረረው የጋዜጠኞችውን አንገት እቆርጣለሁ አለ," *ECADAF Ethiopian News & Opinion*, April 12, 2015, <http://ecadforum.com/Amharic/archives/14790/>.

111 Tedla D. Tekle, "I was forced to drink my own urine": 'Freedom' for netizen after 647 days locked up, but not for all."

112 Tedla D. Tekle, "I was forced to drink my own urine": 'Freedom' for netizen after 647 days locked up, but not for all."

Technical Attacks

Opposition critics and independent voices face frequent technical attacks, even when based abroad. Independent research has found that Ethiopian authorities have used sophisticated surveillance malware and spyware, such as FinFisher's FinSpy and Hacking Team's Remote Control Servers (RCS), to target exiled dissidents.¹¹³

There were no reports of technical attacks against human rights defenders or dissidents during the coverage period, though hacktivists launched attacks on government websites, including the Ministry of Defense, as a form of digital protest alongside the largescale Oromo demonstrations.¹¹⁴ Meanwhile, the Information Network Security Agency (INSA) reported that they had foiled at least 155 cyberattacks in 2015. Critics said they used the data to justify cracking down on the internet.¹¹⁵

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

114 Kinfemichael Yilma, "Hactivism: A New Front of Dissent, Regulation," Addis Fortune, February 14, 2016, <http://addisfortune.net/columns/hactivism-a-new-front-of-dissent-regulation/>

115 "Ethiopia: The cyber attack that probably never was," Zehabesha, July 13, 2016, <http://www.zehabesha.com/ethiopia-the-cyber-attack-that-probably-never-was/>