Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**243**
Land:	Etiopien
Kilde:	Freedom House
Titel:	Freedom on the Net 2014 – Ethiopia
Udgivet:	4. december 2014
Optaget på baggrundsmaterialet:	8. maj 2015

Freedom House

Ethiopia

	2013	2014
Internet Freedom Status	**Not Free**	**Not Free**
Obstacles to Access (0-25)	22	23
Limits on Content (0-35)	28	28
Violations of User Rights (0-40)	29	29
TOTAL* (0-100)	**79**	**80**

* 0=most free, 100=least free

Population:	89.2 million
Internet Penetration 2013:	2 percent
Social Media/ICT Apps Blocked:	Yes
Political/Social Content Blocked:	Yes
Bloggers/ICT Users Arrested:	Yes
Press Freedom 2014 Status:	Not Free

Key Developments: May 2013 – May 2014

- Telecom services worsened, characterized by frequently dropped phone calls, prolonged internet service interruptions, and slow response times to service failures (see **Obstacles to Access**).
- Facebook, Twitter, Yahoo, and CNN were inaccessible for 12 hours in July 2013, while the number of permanently blocked webpages also increased (see **Limits on Content**).
- A law enacted in November 2013 gives the Information Network Security Agency (INSA) carte blanche to inspect private online activities without oversight (see **Violations of User Rights**).
- The government launched sophisticated surveillance malware against several online journalists in the Ethiopian diaspora and dissidents in exile (see **Violations of User Rights**).
- Six bloggers of the prominent Zone9 blogging collective were arrested in April 2014 on charges of terrorism (see **Violations of User Rights**).

Introduction

Ethiopia continues to have one of the lowest rates of internet and mobile phone connectivity in the world, as meager infrastructure, government monopoly over the telecommunications sector, and obstructive telecom policies have significantly hindered the growth of information and communication technologies (ICTs) in the country. Coupled with highly repressive laws and tactics aimed at restricting freedom of expression and access to information, internet freedom in Ethiopia is consistently rated the worst in sub-Saharan Africa and among the worst in the world.

Despite the country's extremely poor telecommunications services and a largely disconnected population, Ethiopia is also known as one of the first African countries to censor the internet, beginning in 2006 with opposition blogs.[1] Since then, internet censorship has become pervasive and systematic through the use of highly sophisticated tools that block and filter internet content and monitor user activity. The majority of blocked websites feature critical news and opposition viewpoints run by individuals and organizations based mostly in the diaspora. Surveillance of mobile phone and internet networks is systematic and widespread, enabled by Chinese-made technology that allows for the interception of SMS text messages, recording of phone calls, and centralized monitoring of online activities. The government also employs commentators and trolls to proactively manipulate the online news and information landscape.

During the report's coverage period, internet freedom in Ethiopia worsened due to increasing restrictions on access to social media and communications tools, such as Storify, and the temporary blocking of Facebook and Twitter in July 2013. A new law passed in November 2013 gave the Information Network Security Agency (INSA) carte blanche to track private online communications and investigate electronic devices without oversight. In addition, a number of diaspora journalists and exiled dissidents were targeted with surveillance malware, demonstrating a growing level of sophistication in the government's effort to silence critical voices that extends beyond the country's borders.

In 2014, the Ethiopian authorities increased their crackdown against bloggers and online journalists, using the country's harsh laws to prosecute individuals for their online activities and quash dissent. Most alarmingly, six bloggers from the critical Zone9 blogging collective and three journalists associated with Zone9 were arrested in late April 2014 on charges of terrorism, which, under the Telecom Fraud Offenses Law and anti-terrorism proclamation, can entail a sentence of up to 20 years in prison if the bloggers are found guilty. The Zone9 case was repeatedly stalled by the courts throughout 2014, leaving the bloggers in pre-trial detention for over six months as of late-2014. Meanwhile, two online radio journalists were arrested and detained for a week without charges in August 2013, and the prominent dissident blogger, Eskinder Nega, and award-winning journalist, Reeyot Alemu, continue to serve lengthy prison sentences, despite international pressure for their release. The overall crackdown has had a major chilling effect on internet freedom and freedom of expression in the country, leading to increasing levels of self-censorship among online journalists, bloggers, and ordinary users alike.

1 Rebecca Wanjiku, "Study: Ethiopia only sub-Saharan Africa nation to filter net," Computerworld, October 8, 2009, http://news.idg.no/cw/art.cfm?id=353092F0-1A64-67EA-E4FBE79C305B60AB.

Obstacles to Access

In 2013 and 2014, access to ICTs in Ethiopia remained extremely limited, hampered by slow speeds and the state's tight grip on the telecom sector.[2] According to the International Telecommunications Union (ITU), internet penetration stood at a mere 1.9 percent in 2013, up from 1.5 percent in 2012.[3] Only 0.25 percent of the population had access to fixed-broadband internet, increasing from 0.01 percent in 2012.[4] Ethiopians had more access to mobile phone services, with mobile phone penetration rates increasing from 22 percent in 2012 to 27 percent in 2013,[5] though such access rates still lag behind a regional average of 80 percent.[6] Meanwhile, less than 5 percent of the population has a mobile-broadband subscription.[7] Radio remains the principal mass medium through which most Ethiopians stay informed.

While access to the internet via mobile phones increased slightly in the last year, prohibitively expensive mobile data packages still posed a significant financial obstacle for the majority of the population in Ethiopia, where per capita income in 2013 stood at US$470.[8] Ethiopia's telecom market is very unsaturated due to monopolistic control, providing customers with few options at arbitrary prices.[9] Prices are set by the state-controlled Ethio Telecom and kept artificially high. As of mid-2014, monthly packages cost between ETB 200 and 3,000 (US$10 to $150) for 1 to 30 GB of 3G mobile services.[10]

The computer remains the most practical option for going online, though in 2014, personal computers are still prohibitively expensive. The combined cost of purchasing a computer, initiating an internet connection, and paying usage charges makes internet access beyond the reach of most Ethiopians. Consequently, only 2 percent of Ethiopian households had internet access in their homes in 2013.[11] The majority of internet users rely on cybercafes to log online, leading to a growth of cybercafes in recent years, particularly in large cities. 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 cybercafes are more expensive.

For the few Ethiopians who can access the internet, connection speeds are known to be painstakingly slow. For years, logging into an email account and opening a single message could take as long as

2 Tom Jackson, "Telecoms slow down development of Ethiopian tech scene – iceaddis," *humanipo*, October 22, 2013, http://www.humanipo.com/news/34843/telecoms-slow-down-development-of-ethiopian-tech-scene-iceaddis/.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2013," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

4 International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2013."

5 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2013."

6 John Koetsier, "African mobile penetration hits 80% (and is growing faster than anywhere else)," *Venture Beat*, December 3, 2013, http://venturebeat.com/2013/12/03/african-mobile-penetration-hits-80-and-is-growing-faster-than-anywhere-else/.

7 International Telecommunication Union, "Ethiopia Profile (Latest data available: 2013)," *ICT-Eye*, accessed August 1, 2014.

8 World Bank, "Ethiopia Overview," last updated July 21, 2014, http://www.worldbank.org/en/country/ethiopia/overview.

9 "Ethiopia – Telecoms, Mobile, Broadband and Forecasts," Paul Budde Communication Pty Ltd. June 2014, http://www.researchandmarkets.com/reports/1222503/ethiopia_telecoms_mobile_broadband_and.

10 Ethio Telecom's Facebook page, post on September 7, 2014, accessed October 1, 2014, https://www.facebook.com/permalink.php?story_fbid=1501293840115809&id=1435268306718363.

11 International Telecommunication Union, "Ethiopia Profile (Latest data available: 2013)," *ICT-Eye*, accessed August 1, 2014, http://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=77.

six minutes at a standard cybercafe with broadband in the capital city.[12] According to May 2014 data from Akamai's "State of the Internet" report, Ethiopia has an average connection speed of 1.2 Mbps (compared to a global average of 3.9 Mbps).[13] Meanwhile, Ethiopia's broadband adoption (characterized by connection speeds greater than 4 Mbps) is less than 3 percent,[14] while the country's narrowband adoption (connection speed below 256 Kbps) is about 20 percent among those with access.[15] Numerous users reported that internet and text messaging speeds were extremely slow during the coverage period, with services completely unavailable at times.[16] Frequent electricity outages are also a contributing factor to poor telecom services.

Despite reports of massive investments from Chinese telecom companies in recent years,[17] Ethiopia's telecommunications infrastructure is among the least developed in Africa and is almost entirely absent from rural areas, where about 85 percent of the population resides. The country is connected 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. In an effort to expand connectivity, the government has reportedly installed several thousand kilometers of fiber-optic cable throughout the country over the past few years.[18] Construction of the East African Submarine Cable System (EASSy) was completed and launched in July 2010, but its effects on Ethiopia have yet to be seen as of mid-2014.[19]

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited,[20] with state-owned Ethio Telecom holding a firm monopoly over internet and mobile phone services in the country. Consequently, all connections to the international internet are completely centralized via Ethio Telecom, enabling the government to cut off the internet at will. As a result, the internet research company Renesys classified Ethiopia "as being at severe risk of Internet disconnection," alongside Syria, Uzbekistan, and Yemen in a February 2014 assessment.[21] During the coverage period, one Renesys report found that 40 percent of Ethiopia's networks were down for a few hours on July 18, 2013 as a result of a disruption on the SEACOM network, though the exact reason for the disruption was unknown.[22] In September 2013, a number of cybercafe owners in Ethiopia reported an increasing trend of unpredictable internet connections and speeds beginning in June that result-

12 Kebena, "Internet Access in the Capital of Africa, Addis Ababa," video, EthioTube.net, posted June 19, 2010, last accessed August 1, 2014, http://www.ethiotube.net/video/9655/Internet-Access-in-the-Capital-of-Africa-Addis-Ababa.

13 Akamai, "Average Connection Speed: Ethiopia," map visualization, *The State of the Internet Q1* (2014), http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

14 Akamai, "Broadband Adoption (connections to Akamai >4 Mbps): Ethiopia," map visualization, *The State of the Internet,* Q1 2014, http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

15 Akamai, "Narrowband Adoption (connections to Akamai <256 kbps): Ethiopia," map visualization, *The State of the Internet,* Q1 2014, http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

16 Bewket Abebe, "Internet Connection Grief," *Addis Fortune*, September 29, 2013, http://allafrica.com/stories/201310020838.html?viewall=1.

17 Aaron Maasho, "Ethiopia signs $700 mln mobile network deal with China's Huawei," *Reuters*, July 25, 2013, http://www.reuters.com/article/2013/07/25/ethiopia-mobile-huawei-idUSL6N0FV4WV20130725.

18 Bewket Abebe, "Internet Connection Grief," *Addis Fortune*, September 29, 2013.

19 Brian Adero, "WIOCC-EASSy Cable Ready for Business," *IT News Africa*, July 23, 2010, http://www.itnewsafrica.com/?p=8419.

20 Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," *Telecentre Magazine*, September 2008, http://bit.ly/16DdF6Z.

21 Jim Cowie, "Syria, Venezuela, Ukraine: Internet Under Fire," Renesys (blog), February 26, 2014, http://www.renesys.com/2014/02/internetunderfire/.

22 Renesys, Twitter post, July 18, 2013, 5:10pm, https://twitter.com/renesys/status/357955490237513729/photo/1.

ed in a significant decline in business, with internet connections reported as unavailable for up to 15 days in a month.[23]

Mobile phone networks—also completely centralized under Ethio Telecom—are similarly vulnerable to service disruptions and shutdowns by the government, which often occur during politically sensitive times. During the coverage period, there were frequent reports of dropped cell phone and landline calls, complete network blackouts in many parts of the country,[24] and overlapping voices in calls. The latter phenomenon led people to suspect government engagement in a widespread eavesdropping scheme (see "Violations of User Rights" for details on surveillance).

Meanwhile, cybercafes are subject to onerous requirements under the 2002 Telecommunications (Amendment) Proclamation,[25] which requires cybercafe owners to obtain an operating license with Ethio Telecom via a murky process that can take months. During the coverage period, Ethio Telecom began enforcing its licensing requirements more strictly in response to the increasing spread of cybercafes, reportedly penalizing Muslim cafe owners more harshly. Violations of the stringent requirements, such as a prohibition on providing Voice-over-IP (VoIP) services, entail criminal liability.[26]

Despite repeated international pressure to liberalize telecommunications in Ethiopia, the government has not eased its grip on the sector.[27] In June 2013, the prime minister publicly affirmed that the government would maintain a monopoly over the country's telecoms.[28] In the meantime, China has emerged as a key investor and contractor in Ethiopia's telecommunications industry,[29] and in July 2013, the government signed a US$1.6 billion agreement with the Chinese telecom companies, Zhongxing Telecommunication Corporation (ZTE) and Huawei, to upgrade its broadband network to 4G in Addis Ababa and expand 3G across the country.[30] The networks built by the Chinese firms have been criticized for their high costs and poor service,[31] though the partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector.[32] Furthermore, the contracts

23 Bewket Abebe, "Internet Connection Grief," *Addis Fortune*, September 29, 2013.

24 Yonas Abiye, "Network Blackout Hits Addis As Parliament Slams Ethio Telecom," *The Reporter*, February 8, 2014, http://allafrica.com/stories/201402102129.html.

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

26 Ethiopian Telecommunication Agency, "License Directive for Resale and Telecenter in Telecommunication Services No. 1/2002," November 8, 2002, accessed August 4, 2014 http://bit.ly/1pUtpWh.

27 "US urge Ethiopia to Liberalise Telecom Sector," *Africa News* via *Somali State*, March 10, 2010, http://www.somalistate.com/englishnewspage.php?articleid=4638; Technology Strategies International, "ICT Investment Opportunities in Ethiopia—2010," March 1, 2010, http://bit.ly/1bmsGvq.

28 "Ethio Telecom to remain monopoly for now," *TeleGeography*, June 28, 2013, http://www.telegeography.com/products/commsupdate/articles/2013/06/28/ethio-telecom-to-retain-monopoly-for-now/.

29 "Ethiopia's Ethio Telecom signs deal with China's ZTE," BBC, August 19, 2013, http://www.bbc.co.uk/news/world-africa-23754626.

30 "Out of reach," *The Economist*, August 24, 2013, http://www.economist.com/news/middle-east-and-africa/21584037-government-expands-mobile-phone-network-tightens-its-grip-out-reach.

31 Matthew Dalton, "Telecom Deal by China's ZTE, Huawei in Ethiopia Faces Criticism," *The Wall Street Journal*, January 6, 2014, http://online.wsj.com/news/articles/SB10001424052702303653004579212092223818288.

32 "Out of reach," *The Economist*, August 24, 2013.

have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust internet and mobile phone censorship and surveillance capacities.[33]

The Ethiopian Broadcasting Authority (EBA) and the Ethiopian Telecommunications Agency (ETA) are the primary regulatory bodies overseeing the telecommunications sector. These two organizations were established as autonomous federal agencies, but both are highly controlled government bodies.

Limits on Content

During the coverage period, over a hundred websites remained inaccessible in Ethiopia, with a greater number of online tools and services targeted for blocking. A June 2014 report affirmed the government's efforts to recruit and train progovernment citizens to attack politically objectionable content online.

The Ethiopian government imposes nationwide, politically motivated internet blocking and filtering that tends to tighten ahead of sensitive political events. The majority of blocked websites are those that feature opposition or critical content run by individuals or organizations based in the country or the diaspora. The government's approach to internet filtering generally entails hindering access to a list of specific internet protocol (IP) addresses or domain names at the level of the Ethio Telecom-controlled international gateway. A more sophisticated strategy of blocking websites based on a keyword in the URL path, known as deep-packet inspection (DPI),[34] was detected in May 2012 when the Tor network—an online tool that enables users to browse anonymously—was blocked.[35]

In January 2014, an independent test conducted by a researcher based in the country found 120 unique URLs that were inaccessible in the country, 62 of which were Ethiopian news websites, 14 of which were political party websites, 37 of which were blogs, and 7 of which were television and online radio websites.[36] During the test, some websites opened at the first attempt but were inaccessible when refreshed. The test also found that select tools and services on Google's Android operating system on smart phones were inaccessible at irregular intervals but for unclear reasons. A separate test on over 1,400 URLs between July and August 2013 by the OpenNet Initiative in partnership with

33 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: "China Involved in ESAT Jamming," *Addis Neger*, June 22, 2010, http://addisnegeronline.com/2010/06/china-involved-in-esat-jamming/, Gary Sands, "Ethiopia's Broadband Network – A Chinese Trojan Horse?" *Foreign Policy Association*, September 6, 2013, http://foreignpolicyblogs.com/2013/09/06/ethiopias-broadband-network-a-chinese-trojan-horse/.

34 Daniel Berhane, "Ethiopia's Web Filtering: Advanced Technology, Hypocritical Criticisms, Bleeding Constitution," *Daniel Berhane's Blog*, January 16, 2011, http://danielberhane.wordpress.com/2011/01/16/ethiopias-web-filtering-advanced-technology-hypocritical-criticisms-bleeding-constitution/.

35 "Ethiopia Introduces Deep Packet Inspection," *Tor*, May 31, 2012, https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection; Warwick Ashford, "Ethiopian Government Blocks Tor Network Online Anonymity," *Computer Weekly*, June 28, 2012, http://www.computerweekly.com/news/2240158237/Ethiopian-government-blocks-Tor-Network-online-anonymity.

36 Test conducted by an anonymous researcher contracted by Freedom House.

Human Rights Watch similarly found 62 websites blocked altogether and numerous others intermittently inaccessible.[37]

International news outlets were increasingly targeted for censorship. Al Arabiya, a Saudi Arabia-based media outlet, and both of Al Jazeera's Arabic and English websites were intermittently blocked during the coverage period.[38] In July 2013, websites belonging to Yahoo and CNN were reportedly inaccessible for about 12 hours. Facebook and Twitter were also targets of the short-term July 2013 blocking.[39] There was no evident impetus or reason for the short-term blocking, and other major services such as Gmail and new outlets such as the New York Times remained accessible. Nevertheless, the incident further increased worries over reports of government plans to block popular social media tools completely.[40] Facebook and Twitter platforms were otherwise generally accessible, although some individual Facebook groups belonging to opposition individuals remained blocked altogether, particularly when accessed via the unencrypted (http://) URL pathway. Meanwhile, the social media curation tool Storify—first blocked in July 2012[41]—remained blocked during the coverage period,[42] while the URL shortening tool Bit.ly was inexplicably blocked in late 2013.[43]

In the past few years, the authorities have become more sophisticated in their censorship techniques, electing to block select webpages as opposed to entire websites. Critical online news articles are usually targeted, such as an August 2012 Forbes article titled, "Requiem for a Reprobate Ethiopian Tyrant Should Not Be Lionized," which was blocked for criticizing the local and global praise of the former prime minister's debatable economic growth achievements; the article remained blocked as of June 2014.[44] A July 2013 YouTube video of the antigovernment Muslim protests that occurred from 2012-13 was also blocked as of late 2013.[45]

International blog-hosting platforms such as Blogspot have been frequently blocked since the disputed parliamentary elections of 2005, during which the opposition used online communication tools to organize and disseminate information that was critical of the ruling Ethiopian People's Revolutionary Democratic Front.[46] In 2007, the government instituted a blanket block on the domain

37 "Citizen Lab collaborates with Human Rights Watch on Internet censorship testing in Ethiopia," Citizen Lab (blog), April 16, 2014, https://citizenlab.org/2014/04/citizen-lab-collaborates-human-rights-watch-internet-censorship-testing-ethiopia/. "Ethiopia 2013 Testing Results," Citizen Lab (Google Drive document), accessed September 8, 2014, https://docs.google.com/spreadsheet/pub?key=0Ah0XQ-1IDRPYdE9JYzBPNWZudEdXMXl4VVk0TC1JNXc&gid=0.

38 "Ethiopia 'Blocks' Al Jazeera Websites," *Al Jazeera*, March 18, 2013, http://www.aljazeera.com/news/africa/2013/03/201331793613725182.html.

39 Websites blocked were all reportedly accessible via proxy servers. See: "Twitter and Facebook Access Restored After 12-Hour Blackout," *OPride*, July 19, 2013, http://www.opride.com/oromsis/news/horn-of-africa/3685-twitter-and-facebook-blocked-in-ethiopia.

40 An old Amharic saying that demonstrates the country's deep-rooted culture of fear —"Stay away from electricity and politics"—recently evolved to: "Stay away from Social Media." The contemporary saying implies that giving one's political opinions via social media could cause grave bodily injury similar to exposing oneself to electricity.

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

42 Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," *Columbia Journalism Review*, August 13, 2012, http://www.cjr.org/behind_the_news/ethiopia_news_crackdown.php?page=all.

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

44 Research conducted by Freedom House consultant.

45 Human Rights Watch, "They Know Everything We Do," March 2014, pg 57, http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf.

46 Bogdan Popa, "Google Blocked in Ethiopia," *Softpedia*, May 3, 2007, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml.

names of two popular blog-hosting websites, Blogspot and Nazret, though the authorities have since become more sophisticated in their censorship techniques, now blocking select pages such as the Zone9 independent blog hosted on Blogspot,[47] as opposed to the entire blogging platform. Nazret, however, remained completely blocked as of June 2014. Circumvention strategies have also been targeted, with the term "proxy" yielding no search results on Google,[48] according to an independent source. Meanwhile, the terms "sex" or "porn" are still searchable.

In addition to increasing blocks of online content, 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. Some restrictions are also placed on mobile phones, such as the requirement for a text message to obtain prior approval from Ethio Telecom if it is to be sent to more than ten recipients.[49] A bulk text message sent without prior approval is automatically blocked.

There are no procedures for determining which websites are blocked or why, which precludes 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. This lack of transparency is exacerbated by the government's continued denial of its censorship efforts. Meanwhile, 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), Ethio Telecom, and the ministry of ICT—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking.

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. Local newspapers and web outlets receive their news and information from regime critics and opposition organizations in the diaspora. While the domestic Ethiopian blogosphere has been expanding, most blogging activity on Ethiopian issues still originates in the diaspora. Few Ethiopian journalists work for both the domestic print media and overseas online outlets due to the threat of repercussions.

Increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly following the arrest of the Zone9 bloggers in April 2014 (see "Violations of User Rights"). Fear of pervasive surveillance has led to widespread self-censorship, and many bloggers publish anonymously to avoid reprisals.[50] Notably, users on social media platforms such as Facebook and Twitter seem to practice a lower degree of self-censorship, which may be due to poor awareness of privacy settings, or the perception that posts on social media are anonymous or more secure.

47 Zone9 blog hosted at: http://zone9ethio.blogspot.com/.

48 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 2014, pg 56, 58.

49 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.

50 Markos Lemma, "Disconnected Ethiopian Netizens," *Digital Development Debates*(blog), http://www.digital-development-debates.org/issues/09-prejudice/african-innovation/disconnected-ethiopian-netizens/.

Despite extremely low levels of internet access, the authorities employ progovernment commentators and trolls to proactively manipulate the online news and information landscape. Acrimonious exchanges between commentators on apologist websites and an array of diaspora critics and opposition figures have become common in online political debates. There was a noticeable increase in the number of progovernment commentators during the coverage period, as confirmed in a June 2014 report by the Ethiopian Satellite Television Service (ESAT) that detailed the government's efforts to recruit and train progovernment citizens to attack politically objectionable content online. According to the ESAT report, hundreds of bloggers who report directly to government officials had been trained on how to post progovernment comments and criticize antigovernment articles on social media platforms.[51]

As the country prepares for the upcoming 2015 National Election, the state media has stepped up its campaign against the press in general and the use of social media in particular, claiming that foreign agents and terrorists are using social media to destabilize the country. Consequently, many civil society groups based in the country are wary of mobilizing against the government, and calls for protest come mostly from the Ethiopian diaspora rather than from local activists who fear the government's violent crackdowns against protest movements.

Nevertheless, over the past few years, Facebook has become one of the most popular mediums through which Ethiopians share and consume information. Social media services have also become significant platforms for political deliberation and social justice campaigns. For example, in September 2013, a group of young Ethiopian bloggers and activists based in Addis Ababa launched a Facebook and Twitter campaign on the occasion of Ethiopia's New Year celebration to share their vision of a better Ethiopia, using the hashtag #EthiopianDream.[52] In November 2013, Ethiopians responded to the Saudi government's crackdown on undocumented Ethiopian immigrants in Saudi Arabia by organizing the online campaign, #SomeoneTellSaudiArabia, to protest the abusive treatment of Ethiopian immigrants.[53]

Netizen activism was particularly pronounced and widespread following the arrest of six Zone9 bloggers and three journalists for their alleged affiliation with the Zone9 collective (see "Violations of User Rights"). Ethiopian bloggers and social media users flocked online to spread the #FreeZone9Bloggers hashtag in a campaign that quickly swept across the social media sphere and garnered widespread support from around the world. Within five days, the #FreeZone9Bloggers hashtag had been tweeted more than 8,000 times.[54] Unfortunately, the international campaign elicited no response from the government, and the imprisoned bloggers and journalists are still awaiting trial on charges of terrorism as of late-2014.

51 "Ethiopia Trains Bloggers to attack its opposition," *ECADF Ethiopian News & Opinions*, June 7, 2014, http://ecadforum.com/2014/06/07/ethiopia-trains-bloggers-to-attack-its-opposition.

52 Selamawit, "Millions of Ethiopians share their dream for our country in the new year. What is your dream?" *Sodere*, September 6, 2013, http://sodere.com/profiles/blogs/millions-of-ethiopians-share-their-dream-for-their-country-in-the.

53 Ndesanjo Macha, "Ethiopians: #SomeoneTellSaudiArabia to Stop Immigration Crackdown," Global Voices (blog,) November 13, 2013, http://globalvoicesonline.org/2013/11/13/ethiopians-someonetellsaudiarabia-to-stop-immigration-crackdown/.

54 "#BBCtrending: Jailed bloggers spark Ethiopia trend," *BBC Trending*, April 30, 2014, http://www.bbc.com/news/blogs-trending-27212472.

Violations of User Rights

During the coverage period, the Ethiopian government's already limited space for online expression continued to deteriorate alongside its poor treatment of journalists. A new proclamation passed in November 2013 empowered INSA with sweeping surveillance capabilities without judicial oversight. Sophisticated malware was launched against online radio journalists and dissidents in exile, while repression against bloggers and ICT users in the country increased notably. Six bloggers of the critical Zone9 blogging collective were arrested for their alleged terrorist activities.

The 1995 Ethiopian constitution guarantees freedom of expression, freedom of the press, and access to information, while also prohibiting censorship.[55] These constitutional guarantees are affirmed in the 2008 Mass Media and Freedom of Information Proclamation, known as the press law, which also provides certain protections for media workers, such as prohibiting the pre-trial detention of journalists.[56] Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression. For example, media outlets are required to obtain licenses to operate through an onerous registration process that applies to all outlets, regardless of size, though it is uncertain whether the press law's broad language encompasses online media.[57] Penalties for violating the registration requirement and other restrictions on content, such as defamation, involve high fines and up to two and three years in prison, respectively.[58]

In September 2012, the government codified specific restrictions on various telecommunications activities through the passage of the Telecom Fraud Offences law,[59] which revised a 1996 law that had placed bans on certain communication applications, such as Voice over Internet Protocol (VoIP)[60]—including Skype and Google Voice—call back services, and internet-based fax services.[61] Under the new law, the penalties under the preexisting ban were toughened, increasing the fine and maximum prison sentence from five to eight years for offending service providers, and penalizing users with three months to two years in prison.[62] The law also added the requirement for all individuals to register their telecommunications equipment—including smart phones—with the government, which security officials typically enforce by confiscating ICT equipment when a registration permit cannot be furnished at security checkpoints, according to sources in the country.

55 Constitution of the Federal Democratic Republic of Ethiopia (1995), articles 26 and 29, accessed August 24, 2010, http://www.ethiopar.net/.

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

57 Article 19, "The Legal Framework for Freedom of Expression in Ethiopia," accessed September 10, 2014, http://www.article19.org/data/files/pdfs/publications/ethiopia-legal-framework-for-foe.pdf.

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

59 "A Proclamation on Telecom Fraud Offence," *Federal Negarit Gazeta* No. 61, September 4, 2012, http://www.abyssinialaw.com/uploads/761.pdf.

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

61 Ethiopian Telecommunication Agency, "Telecommunication Proclamation No. 281/2002, Article 2(11) and 2(12)," July 2, 2002, accessed July 25, 2014, http://www.researchictafrica.net/countries/ethiopia/Telecommunications_(Amendment)_Proclamation_no_281;2002.pdf. As an amendment to article 24 of the Proclamation, the Sub-Article (3) specifically states, "The use or provision of voice communication or fax services through the internet are prohibited" (page 1782).

62 A Proclamation on Telecom Fraud Offence.

Most alarmingly, the Telecom Fraud Offences law extended the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and 2004 Criminal Code to electronic communications, which are broadly defined yet explicitly include both mobile phone and internet services.[63] The anti-terrorism 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, vaguely defined.[64] Meanwhile, the criminal code holds any "author, originator or publisher" criminally liable for content allegedly linked to offenses such as treason, espionage, or incitement, which carries with it the penalty of up to life imprisonment or death.[65] The criminal code also penalizes the publication of a "false rumor" with up to three years in prison.[66]

In 2014, the Ethiopian authorities increased their crackdown against bloggers and online journalists, using the country's harsh laws to prosecute individuals for their online activities and silence dissent. Most alarmingly, six bloggers from the critical Zone9 blogging collective and three journalists associated with Zone9 were arrested in late April 2014 on charges of terrorism. They were accused of "working with foreign organizations that claim to be human rights activists… and receiving finance to incite public violence through social media,"[67] though the arrests had occurred just days following Zone9's Facebook post announcing plans to resume its activism. The blogging collective had been inactive for seven months as a result of "a considerable amount of surveillance and harassment" the bloggers had suffered at the hands of security agents for their writings and social media activism.[68] Despite widespread international condemnation of the Zone9 arrests, the detainees were denied bail in August and remained in jail as of fall 2014, awaiting trial.[69] Meanwhile, the well-known dissident journalist and blogger Eskinder Nega is still carrying out an 18-year prison sentence handed down in July 2012 under the anti-terrorism law.[70]

Numerous other journalists and media outlets—both online and print—were targeted for arrest and prosecutions during the coverage period, including Darsema Sori and Khalid Mohammed who were arrested in August 2013 for their work with the online radio station, Radio Bilal, which is known for its extensive coverage of the 2012-13 antigovernment protests organized by Ethiopian Muslims.

63 Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences."

64 "Anti-Terrorism Proclamation No. 652/2009," *Federal Negarit Gazeta* No. 57, August 28, 2009.

65 International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Article 44," http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf.

66 "The Criminal Code of the Federal Democratic Republic of Ethiopia.'

67 "Six Members of Blogging Collective Arrested in Ethiopia," Global Voices Advocacy, April 26, 2014, http://advocacy.globalvoicesonline.org/2014/04/26/six-members-of-blogging-collective-arrested-in-ethiopia/.

68 Six members of Zone Nine, group of bloggers and activists are arrested" [in Amharic], Zone9 (blog), April 25, 2014, http://zone9ethio.blogspot.com/2014/04/9.html.

69 "Nine Journalists and Bloggers Still Held Arbitrarily," Reporters Without Borders, August 21, 2014, http://en.rsf.org/ethiopia-nine-journalists-and-bloggers-21-08-2014,46830.html.

70 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. Sarah Hoffman, "That Bravest and Most Admirable of Writers: PEN Salutes Eskinder Nega," PEN American Center (blog), April 13, 2012, http://www.pen.org/blog/?p=11198. See also, Markos Lemma, "Ethiopia: Online Reactions to Prison Sentence for Dissident Blogger," *Global Voices*, July 15, 2012, http://globalvoicesonline.org/2012/07/15/ethiopia-online-reactions-to-prison-sentence-for-dissident-blogger/; Endalk, "Ethiopia: Freedom of Expression in Jeopardy,' *Global Voices*, February 3, 2012, http://advocacy.globalvoicesonline.org/2012/02/03/ethiopia-freedom-of-expression-in-jeopardy/.

They were released after being held for a week without charges,[71] but the arrests were in keeping with the government's concerted efforts to silence the protests.

Given the high degree of online repression in Ethiopia, some political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent filtering, though the ability to communicate anonymously has become more difficult. The Tor Network anonymizing tool was blocked in May 2012, confirming that the government has deployed deep-packet inspection technology, and Google searches of the term "proxy" mysteriously yield no results.

Anonymity is further compromised by strict SIM card registration requirements. Upon purchase of a SIM card through Ethio Telecom or an authorized reseller, individuals must provide their full name, address, government-issued identification number, and a passport-sized photograph. Ethio Telecom's database of SIM registrants enables the government to cut-off the SIM cards belonging to targeted individuals and to restrict those individuals from registering for new SIM cards. Internet subscribers are also required to register their personal details, including their home address, with the government. In 2013, an inside informant leaked worrying details of potential draft legislation that seeks to mandate real-name registration for all internet users in Ethiopia, though there are no further details of this development as of mid-2014.[72]

Government surveillance of online and mobile phone communications is pervasive in Ethiopia, and evidence has emerged in recent years that reveal the scale of such practices. According to 2014 Human Rights Watch research, there are strong indications that the government has deployed a centralized monitoring system from the Chinese telecommunications firm ZTE, known as ZXMT, to monitor phone lines and various types of communications, including mobile phone networks and the internet.[73] Known for its use by repressive regimes in Libya and Iran, ZXMT enables deep-packet inspection (DPI) of internet traffic 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.[74] ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.[75] 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.[76]

In November 2013, a new Cyber Security Law expanded the surveillance powers of the Information Network Security Agency (INSA)—the government body established in 2011 to preside over the se-

71 "Two Ethiopian journalists held for a week without charge," CPJ (news alert), August 9, 2013, http://cpj.org/2013/08/two-ethiopian-journalists-held-for-a-week-without.php.

72 Interview conducted by Freedom House consultant.

73 Human Rights Watch, "They Know Everything We Do," March 2014, pg 62, http://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf.

74 Human Rights Watch, "They Know Everything We Do," March 2014, pg 67.

75 Human Rights Watch, "They Know Everything We Do," March 2014, pg 52.

76 Committee to Protect Journalists, "Ethiopian Blogger, Journalists Convicted of Terrorism," January 19, 2012, http://cpj.org/2012/01/three-journalists-convicted-on-terrorism-charges-i.php.

curity of the country's critical communications infrastructure.[77] According to reports, the law states that "social media outlets, blogs and other internet related media have great capabilities to instigate war, to damage the country's image and create havoc in the economic atmosphere of the country"—setting the logic for expanding INSA's duties to include developing offensive cyber capabilities and ICT tools. The proclamation also empowers INSA to investigate computers, networks, internet, radio, television, and social media platforms "for any possible damage to the country's social, economic, political and psychological well being."[78]

INSA reportedly uses sophisticated spyware, such as the commercial toolkit FinFisher—a device that can secretly monitor computers by turning on webcams, record everything a user types with a key logger, and intercept Skype calls—to target dissidents and supposed threats.[79] A leaked document confirmed that the UK-based company, Gamma International, had provided Ethio Telecom with the FinFisher surveillance toolkit at some point between April and July 2012.[80] In addition, research conducted by Citizen Lab in March 2013 worryingly found evidence of an Ethio Telecom-initiated FinSpy campaign launched against users that employed pictures of the exiled prodemocracy group, Ginbot 7, as bait.[81]

There has been an increasing trend of exiled dissidents targeted with surveillance malware in the past few years. In April 2013, Tadesse Kersmo, a senior member of Ginbot-7 living in exile in the United Kingdom since 2009, came across the above-mentioned Citizen Lab FinSpy report and noticed that one of the spyware campaign's bait was a picture of himself.[82] He contacted Citizen Lab to have his computer examined and found that FinSpy had been active on his computer over two days in June 2012.[83] The spyware may have transmitted any or all of Kersmo's emails, chats, Skype calls, files, and web searches to a server based in Ethiopia, which could have provided the authorities with names of contacts, colleagues, and family members still living in the country.[84] In February 2014, Privacy International filed a criminal complaint to the UK's National Cyber Crime Unit on Kersmo's behalf, urging them to investigate the potential unlawful interception of communications.

In the same month, the Electronic Frontier Foundation filed a similar suit in the United States on behalf of another Ethiopian dissident (and American citizen) identified publicly under the pseudonym

77 Yonas Abiye, "INSA to reign all-powering cyberspace," *The Reporter*, November 9, 2013, http://www.thereporterethiopia.com/index.php/news-headlines/item/1217-insa-to-reign-all-powerful-over-cyberspace.

78 "Informationa Network Security Agency (INSA) of Ethiopia is to be reestablished," *Dire Tube*, November 5, 2013, http://www.diretube.com/articles/read-information-network-security-agency-insa-of-ethiopia-is-to-be-reestablished_3833.html#.UyDWIPldVz4.

79 Fahmida Y. Rashid, "FinFisher 'Lawful Interception' Spyware Found in Ten Countries, Including the U.S.," *Security Week*, August 8, 2012, http://www.securityweek.com/finfisher-lawful-interception-spyware-found-ten-countries-including-us.

80 The document was seen by Freedom House consultant. Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab (University of Toronto), March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

81 Marquis-Boire, "You Only Click Twice."

82 Liat Clark, "Ethiopian refugee 'illegally' spied on using British software," *Wired*, February 17, 2014, http://www.wired.co.uk/news/archive/2014-02/17/illegal-spying-ethiopian-refugee.

83 "Privacy International seeking investigation into computer spying on refugee in UK," Privacy International (press release), February 17, 2014, https://www.privacyinternational.org/press-releases/privacy-international-seeking-investigation-into-computer-spying-on-refugee-in-uk; Liat Clark, "Ethiopian refugee 'illegally' spied on using British software."

84 Joshua Kopstein, "Hackers Without Borders," *The New Yorker*, March 10, 2014, http://www.newyorker.com/online/blogs/elements/2014/03/hacked-by-ones-own-government.html.

Mr. Kidane.[85] Kidane's computer had also been found infected with the FinSpy malware sometime between late October 2012 and March 2013, which had secretly recorded dozens of his Skype calls, copied emails he had sent, and logged a web search conducted by his son on the history of sports medicine for a school research project.[86] The FinSpy IP address was linked to a server belonging to Ethio Telecom.

Recent Citizen Lab research published in February 2014 uncovered the use of Remote Control System (RCS) spyware against two employees of the diaspora-run independent satellite television, radio, and online news media outlet, Ethiopian Satellite Television Service (ESAT), based in Alexandria, VA.[87] 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/chats.[88] While Hacking Team claims that they do not deal with "repressive regimes,"[89] the RCS virus sent via sophisticated bait to the two ESAT employees made it clear that the attack was targeted, and researchers have strong suspicions of the Ethiopian government's involvement.[90]

While the government's stronghold over the Ethiopian ICT sector enables it to proactively monitor users, its access to user activity and information is less direct at cybercafes. For a period following the 2005 elections, cybercafe owners were required to keep a register of their clients, but the requirement has not been enforced since mid-2010.[91] Nevertheless, some cybercafe operators revealed that they are required to report any "unusual behavior" to security officials, and officials often visit cybercafes (sometimes in plainclothes) to ask questions about specific users or monitor user activity themselves.[92]

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 claim that they are consistently threatened by state security agents for their online activism. Bloggers from Zone9, for example, reported suffering a considerable amount of harassment for their work, leading them to go silent for several months. Shortly after the blog announced on Facebook that it was resuming activities in April 2014, six Zone9 bloggers were arrested and sent to a federal detention center in Addis Ababa where the torture of detainees is reportedly common.[93] The active Gmail accounts belonging to sev-

85 "American Sues Ethiopian Government for Spyware Infection," Electronic Frontier Foundation (press release), February 18 2014, https://www.eff.org/press/releases/american-sues-ethiopian-government-spyware-infection.

86 "Kidane v. Ethiopia," Electronic Frontier Foundation, last updated August 28, 2014, https://www.eff.org/cases/kidane-v-ethiopia.

87 Bill Marczak et al., "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/.

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

89 Declan McCullagh, "Meet the 'Corporate Enemies of the Internet' for 2013," *CNET*, March 11, 2013, accessed February 13, 2014, http://news.cnet.com/8301-13578_3-57573707-38/meet-the-corporate-enemies-of-the-internet-for-2013/.

90 Craig Timberg, "Foreign regimes use spyware against journalists, even in U.S.," *Washington Post*, February 12, 2014, http://wapo.st/McG3TZ.

91 Groum Abate, "Internet Cafes Start Registering Users," *Capital*, December 25, 2006, http://www.capitalethiopia.com/index.php?option=com_content&view=article&id=259:internet-cafes-start-registering-users-&catid=12:local-news&Itemid=4.

92 Human Rights Watch, "They Know Everything We Do," March 2014, pg 67.

93 "Timeline," Zone9ers 'Trial' (blog), April 26, 2014, http://trialtrackerblog.org/press/.

eral of the Zone9 bloggers[94] while in detention suggests that they may have been forced give their passwords to security officials against their will.

94 Anonymous Freedom House researcher reported seeing several of the detained Zone9 bloggers actively online in Gmail chat.