የወያኔ መንግስት ስልክና ኢንተርኔት ላይ የሚያደርገውን ቁጥጥር፣ በዜጎች ላይ የሚፈፅመውን አፈና እና እስር፤ የሚያሳይ ጥልቅ ሪፖርት

November 7, 2015 – ቆንጅት ስጦታው — Comments ↓

የወያኔ መንግስት ቴሌኮም አገልግሎት በተለይ ስልክና ኢንተርኔት ላይ የሚያደርገውን ቁጥጥር፣ በዜጎች ላይ የሚፈፅመውን አፈና እና እስር፤ በተያያዘም ኢትዮጵያ በቴሌና ኢንተርኔት በአቅርቦት ያለችበትን አነስተኛ ደረጃ የሚያሳይ ጥልቅ ሪፖርት ነው፡፡ በተለይ ማህበራዊ ድረገፅና ቴሌ ኮም ተጠቃሚዎች ላይ የሚደርሰውን አፈና እና የአቅርቦት ችግር በስፋት የዳሰሰ በመሆኑ ሊነበብ ይገባዋል እንላለን፡፡

June 2014—May 2015

• A significant number of service interruptions in the name of routine maintenance and system updates resulted in worsening service across the country. Internet services on 3G mobile internet networks were reportedly unavailable for more than a month in July and August 2014 (see Restrictions on Connectivity).

• A growing number of critical news and opposition websites were blocked in the lead up to the May 2015 elections (see Blocking and Filtering).

• Six bloggers of the prominent Zone 9 blogging collective arrested in April 2014 were officially charged with terrorism in July 2014; two of the bloggers were unexpectedly released and acquitted in July 2015, joined by the four others in October (see Prosecutions and Arrests).

• A university political science teacher known for his Facebook activism and another blogger were arrested and charged with terrorism in July 2014, among three others (see Prosecutions and Arrests).

• Online journalists in the Ethiopian diaspora were attacked with Hacking Team's sophisticated surveillance malware (see Technical Attacks).

Introduction:

Ethiopia, the second most populated country in sub-Saharan Africa, has one of the lowest rates of internet and mobile phone connectivity in the world. Telecommunication services, in general, and the internet, in particular, are among the most unaffordable commodities for the majority of Ethiopians, as poor telecom infrastructure, the government's monopoly over the information and communication technologies (ICTs) sector, and obstructive telecom

policies have significantly hindered the growth of ICTs in the country, making the cost of access prohibitively expensive. 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 in the diaspora. In the lead up to the May 2015 general elections, a growing number of critical news and opposition websites were blocked, while select tools, such as Storify and a popular URL shortening tool Bitly, remained blocked throughout the year. The government also employs commentators and trolls to proactively manipulate the online news and information landscape, and surveillance of mobile phone and internet networks is systematic and widespread.https://freedomhouse.org/report/freedom-net/2015/ethiopia

In 2014–15, the Ethiopian authorities increased their crackdown on bloggers and online journalists, using the country's harsh laws to prosecute individuals for their online activities and quash critical voices. The Zone 9 bloggers arrested in April 2014 were charged with terrorism in July 2014 and subsequently subjected to a series of sham trials through mid-2015. In July 2015, two of the imprisoned Zone 9 bloggers were unexpectedly released and acquitted of all charges, which observers attributed to U.S. President Barack Obama's official visit to the country later that month. The four remaining Zone 9 bloggers were acquitted in October. Nevertheless, five other critical voices and bloggers who were arrested in July 2014 and charged with terrorism remain in prison. During the numerous Zone 9 trials throughout 2014–2015, several supporters were temporarily arrested for posting updates and pictures of their trials on social media via mobile devices.

Obstacles to Access:

A significant number of service interruptions in the name of routine maintenance and system updates resulted in worsening service across the country. Internet services on 3G mobile internet networks were reportedly unavailable for more than a month in July and August 2014.

Availability and Ease of Access

In 2015, 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 3 percent in 2014, up from just 2 percent in 2013.[3] Only 0.5 percent of the population had access to fixed-broadband connections, increasing from 0.25 percent in 2013.[4] Ethiopians had more access to mobile phone services, with mobile phone penetration rates increasing from 27 percent in 2013 to 32 percent in 2014,[5] though such access rates still lag behind an estimated regional average of 74 percent,[6] and cell phone ownership is much more common in urban areas than rural areas. Meanwhile, less than 5 percent of the population has a mobile-broadband subscription as of the latest available data from 2013.[7] In March 2015, Ethiopia's single telecoms provider, the state-owned EthioTelecom, announced it had launched 4GLTE mobile technology in the capital Addis Ababa,[8] but the service is reportedly only available to a mere 400,000 subscribers.[9] Radio remains the principal mass medium through which most Ethiopians stay informed.

While access to the internet via mobile phones increased slightly in the past year, prohibitively expensive mobile data packages still posed a significant financial obstacle for the majority of the population in Ethiopia, where per capita income stood at US$470 as of the latest available data from 2013.[10] Ethiopia's telecom market is highly undeveloped due to monopolistic control, providing customers with few options at arbitrary prices, which are set by the state-controlled EthioTelecom and kept artificially high.[11] As of mid-2015, monthly packages cost between ETB 200 and 3,000 (US$10 to $150) for 1 to 30 GB of 3G mobile services.

The combined cost of purchasing a computer, setting up an internet connection, and paying usage charges makes internet access beyond the reach of most Ethiopians. Consequently, only 2 percent of Ethiopian households have fixed-line internet access in their homes.[12] While access via mobile internet is increasing, the majority of internet users still rely on cybercafes to log online. 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 and have not improved in years, despite rapid improvements everywhere else around the world. Logging into an email account and opening a single message can still take as long as six minutes at a standard cybercafe with broadband in the capital city—the same rate reported over the past few years—while attaching documents or images to an email can take as long as eight minutes or more.[13] According to May 2015 data from Akamai's "State of the Internet" report, Ethiopia has an average connection speed of 1.8 Mbps (compared to a global average of 3.9 Mbps).[14]

Despite reports of massive investments from Chinese telecom companies in recent years,[15] 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. There are only a few signal stations across the country, resulting in frequent network congestions and disconnections, even on state controlled media.[16] Consequently, many people often use their cell phones as music players or cameras. In a typical small town of Ethiopia, individuals often hike to the top of their nearest hills to access a signal for a mobile phone call. Frequent electricity outages also contribute to poor telecom services.

Restrictions on Connectivity

The Ethiopian government's complete control over the country's telecommunications infrastructure via EthioTelecom enables it to restrict access to the internet and mobile phone services. Ethiopia 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. All connections to the international internet are completely centralized via EthioTelecom, 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.[17]

There were a significant number of service interruptions throughout the year in the name of routine maintenance of network infrastructure and system updates across the country, resulting in worsening service. Numerous users reported extremely slow

internet and text messaging speeds during the coverage period, and internet services on EVDO and CDMA networks were reportedly unavailable for more than a month in July and August 2014.[18]
In a sample test conducted in March 2015 to measure the frequency and pervasiveness of mobile network interruptions, 40 to 60 percent of phone calls dropped in the middle of conversation.[19] Nearly 70 percent of the time, testers needed to make prolonged and repeated attempts for their calls to go through. Text messaging services were also found to be extremely poor and slow. The same sample test found that it took an average of six minutes to send a text message to ten individuals, while replies varied from one to six minutes. Approximately 30 percent of text messages were not delivered to the intended recipient at all. The test further found that 60 percent of mobile phone users frequently ran out of their prepaid mobile data allowances prematurely.

ICT Market

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited,[20] 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.[21]
China is a key investor in Ethiopia's telecommunications industry,[22] with Zhongxing Telecommunication Corporation (ZTE) and Huawei currently serving as contractors to upgrade broadband networks to 4G in Addis Ababa and to expand 3G across the country.[23] The partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector,[24] though the networks built by the Chinese firms have been criticized for their high cost and poor service.[25] 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.[26] In December 2014, the Swedish telecom group Ericsson emerged as the latest partner to improve and repair the quality of Ethiopia's mobile network infrastructure,[27] though China's ZTE still maintains the lion's share of the telecom infrastructure investment sector.
Meanwhile, onerous government regulations stymie other aspects of the Ethiopian ICT market. For one, imported ICT items are tariffed at

the same heavy 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.[28] Ethiopians are required register their laptops and tablets at the airport with the Ethiopian customs authority before they travel out of the country, ostensibly to prevent individuals from illegally importing electronic devices, though observers believe the requirement is an effort to keep tabs on the ICT activities of Ethiopian citizens.[29]

Local software companies in the country have also suffered from heavy-handed government regulations, which do not have fair, open, or transparent ways of evaluating and awarding bids for new software projects.[30] 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.

Meanwhile, cybercafes are subject to onerous operating requirements under the 2002 Telecommunications (Amendment) Proclamation,[31] which requires cybercafe owners to obtain an operating license with EthioTelecom via a murky process that can take months. In the past few years, EthioTelecom began enforcing its licensing requirements more strictly in response to the increasing spread of cybercafes, reportedly penalizing Muslim cafe owners more harshly. Violations of the stringent requirements, such as a prohibition on providing Voice-over-IP (VoIP) services, entail criminal liability, though there have been no reported violations to date.[32]

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, executives in the government have complete control over ICT policy and sector regulation.[33] The Information Network Security Agency (INSA), a government agency established in 2011 and controlled by individuals with strong ties to the ruling regime,[34] also has significant power in regulating the internet under the mandate of protecting the country's communications infrastructure and preventing cybercrimes in the country.

Limits on Content:

Dozens of critical news and opposition websites and blogs were

blocked as the country prepared for the general elections in May 2015. Over 100 websites remained blocked overall. The activities of progovernment commentators noticeably increased during the coverage period.

Blocking and Filtering

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 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 piece of communication (such as email).[35]

During the coverage period, over one hundred websites remained inaccessible in Ethiopia.[36] Blocked sites included Ethiopian news websites, political party websites, blogs, television and online radio 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 inaccessible at irregular intervals but for unclear reasons.

Online censorship intensified as the country prepared for the May 2015 general elections, with new blocks on dozens of social media pages, blogs, and diaspora-based opposition websites that were created to report on the general election.[37] A diaspora-operated website called AddisVoice, which published a series of critical articles about the educational qualifications of government officials, was a top target for blocking in 2014-2015.[38] International news outlets were also targeted. In June 2014, the Ethiopian authorities were accused of jamming the satellite operations of the BBC, Deutsche Welle, France 24, and the Voice of America, blocking a few of the stations' websites as well.[39] Al Arabiya, a Saudi Arabia-based media outlet, and Al Jazeera's Arabic and English websites were intermittently blocked throughout the coverage period.[40]

Blogs are also a prime target for blocking. In 2007, the government instituted a blanket block on the domain 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,[41] as opposed to the entire blogging platform. Nazret, however, remained completely blocked as of June 2015. Facebook and Twitter platforms were otherwise generally accessible, although some individual Facebook groups belonging to opposition individuals remained blocked altogether when accessed via the unencrypted (HTTP) URL pathway. However, the social media curation tool Storify—first blocked in July 2012[42]—remained blocked during the coverage period,[43] in addition to the URL shortening tool Bit.ly.[44] Circumvention tools are also blocked, including Tor—an online tool that enables users to browse anonymously—which has been blocked since May 2012.[45] According to an independent source, key terms such as "proxy" yield no search results on unencrypted search engines,[46] reflecting the government's efforts to limit users' access to circumvention tools and strategies.

Some restrictions are also placed on mobile phones, such as the requirement for a text message to obtain prior approval from EthioTelecom if it is to be sent to more than ten recipients.[47] A bulk text message sent without prior approval is automatically blocked, irrespective of the content of the 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. 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), EthioTelecom, and the ICT ministry—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking. 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

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. For instance, during the various legal proceedings of the Zone 9 bloggers throughout 2014-2015 (see "Prosecutions"), friends and reporters who posted pictures and stories of the trials on social media were briefly detained and asked to remove them.[48]

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."[49] Launching a website on the local .et domain is expensive and onerous,[50] requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.[51] While the domestic Ethiopian blogosphere has been expanding, most blogs are hosted on international platforms by diaspora community members.

Despite extremely low levels of internet access, the authorities employ progovernment commentators and trolls to manipulate the online news and information landscape. There was a noticeable increase in the number of progovernment commentators in the last few years, 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 reporting directly to government officials had been trained on how to post progovernment comments and criticize antigovernment articles on social media platforms.[52]

Meanwhile, increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly following the arrest of the Zone 9 bloggers in April 2014 and their ongoing trials throughout 2014-2015 (see "Prosecutions"). Fear of pervasive surveillance has also led to widespread self-censorship, and many bloggers publish anonymously to avoid reprisals.[53] Local newspapers and web outlets receive their independent news and

information from regime critics and opposition organizations in the diaspora, and few Ethiopian journalists work for either domestic print media or overseas online outlets due to the threat of repercussions.

Digital Activism

Despite very low internet penetration in the country, tech-savvy Ethiopians are increasingly using social media for campaigning and social activism. Digital activism was particularly pronounced and widespread following the arrest of six Zone 9 bloggers and three journalists for their alleged affiliation with the Zone 9 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 throughout 2014-2015. In the first five days of the campaign, the #FreeZone9Bloggers hashtag was tweeted more than 8,000 times.[54] While the international campaign elicited no official response from the government, sustained digital activism throughout the year continually informed the international community of the Zone 9 case, pushing high level diplomats to condemn the Ethiopian government's actions, which many believe helped lead to the release of two of the bloggers in July 2015.

Following the prominence of the Zone 9 blogger campaign, hashtag campaigns on social media have become one of the most popular methods of activism in Ethiopia, enabling citizens to demand for social change and justice on a variety of issues. Two hashtag campaigns in late 2014 were particularly active on Ethiopian social media. One campaign, #BecauseIamOromo, stemmed from the release of an Amnesty International report on repression and human rights violations in the Oromo region of Ethiopia,[55] building momentum across a three-day Twitter campaign, which attracted a significant number of followers.[56] Another campaign, #Justice4Hanna, demanded justice for a 16 year old high school girl who was gang-raped and then later died from associated injuries in Addis Ababa in October 2014.[57]

Digital activism was also prominent in the lead-up to the May 2015 general elections, though calls for protest came mostly from the Ethiopian diaspora rather than from local activists who feared the government's violent crackdowns against protest movements. State media stepped up its campaign against the press, in general, and

the use of social media, in particular, claiming that foreign agents and terrorists were using social media to destabilize the country.

Violations of User Rights:

The limited space for online expression continued to deteriorate alongside an increasing crackdown on bloggers. The Zone 9 bloggers arrested in April 2014 were charged with terrorism in July 2014 and subsequently subjected to a series of sham trials through mid-2015. In July 2015, two of the imprisoned Zone 9 bloggers were unexpectedly released and acquitted of all charges, leaving four in prison alongside five other individuals who were arrested in July 2014 and charged with terrorism for their various ICT activities. Independent journalists in the diaspora were targeted with Hacking Team surveillance spyware.

Legal Environment

The 1995 Ethiopian constitution guarantees freedom of expression, freedom of the press, and access to information, while also prohibiting censorship.[58] 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.[59] Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression, such as onerous registration processes for media outlets and high fines for defamation.[60] The Criminal Code also penalizes defamation with a fine or up to one year in prison.[61]

In 2012, the government introduced specific restrictions on an array of ICT activities under amendments to the 1996 Telecom Fraud Offences Law,[62] which had already placed bans on certain communication applications, such as Voice over Internet Protocol (VoIP)[63] like Skype and Google Voice, call back services, and internet-based fax services.[64] Under the 2012 amendments, the penalties under the preexisting ban were toughened, increasing the fine and maximum prison sentence from five to eight years for service providers, and penalizing users with three months to two years in prison.[65] The law also added the requirement for all individuals to register their telecommunications equipment—including smartphones—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.

Most alarmingly, the 2012 Telecom Fraud Offences Law extended

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. [66] 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, a vaguely defined term.[67]

According to a December 2014 news report by Ethiopian State Television, a draft Computer and Internet Crime Bill is currently in the works by the Information Network Security Agency (INSA). The news report featured remarks by the INSA director, who insisted that the draft cybercrime law aimed to strengthen the government's powers to prevent, control, investigate, and prosecute cybercrimes, including on social media. Observers are concerned that the law will empower state agencies to monitor private social media activities without oversight.[68]

Prosecutions and Detention for Online Activities

Ethiopia is among the world's top five jailers of journalists.[69] In 2014-2015, the authorities intensified their crackdown against bloggers and online journalists, using the country's harsh laws to arrest and prosecute individuals for their online activities and silence dissent. Most alarmingly, six bloggers from the critical Zone 9 blogging collective and three journalists with alleged associations to Zone 9 were arrested in late April 2014. The arrests occurred just days following a Facebook post announcing the group's plans to resume its activism after taking a seven-month hiatus due to "a considerable amount of surveillance and harassment" the bloggers had previously suffered at the hands of security agents for their writings and social media activism.[70]

Initially held for three months without charges, the bloggers were charged in July 2014 with terrorism under the harsh Anti-Terrorism Proclamation for conspiring with the banned opposition group Ginbot 7, which the government classifies as a terrorist group.[71] The bloggers were further accused of encrypting their communications to disseminate seditious writings with the intent of overthrowing the government, the latter of which is an offense under the criminal code.[72] The government reportedly submitted 30 pages of phone and surveillance records spanning a period of three years as evidence of the terrorism charges,[73] alongside email communications and digital security handbooks.[74]

Despite widespread international condemnation of the Zone 9 arrests, the detainees were denied bail and brought to court dozens of times without any progress to their case for more than a year.[75] They remained in jail throughout the first half of 2015 until early July, when two of the bloggers and three associated journalists were unexpectedly released without charges. The four remaining Zone 9 bloggers were acquitted in October.[76] During the trials between June and November 2014, at least three other individuals were arrested temporarily for posting updates and pictures of their trials on social media via mobile devices.

Several other critical bloggers and online activists were arrested in July 2014, including Abraha Desta and Zelalem Workagegnehu, both academics and bloggers who were held without charges for four months until October 2014 when they were charged for their alleged support of the opposition group Ginbot 7.[77] They were also charged with using social media to contact members of Ginbot 7.[78] Widely known for his Facebook posts criticizing the ruling party, Abraha Desta was reportedly beaten brutally before being taken to an unidentified prison.[79] Three other individuals—Yonatan Wolde, Abraham Solomon, and Bahiru Degu—were also arrested around the same time for allegedly applying for an internet security and social media training abroad.[80] At a court hearing in August 2015, the defendants' cases were delayed until November.[81]

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.[82]

Surveillance and Anonymity

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.[83] Known for its use by repressive regimes in Libya and Iran, ZXMT 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.[84] ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.[85] 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.[86]

There has been an increasing trend of exiled dissidents targeted with surveillance malware in the past few years (see "Technical Attacks"). Recent Citizen Lab research published in March 2015 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, Virginia, in November and December 2014.[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, as well as to intercept Skype calls and chats. [88]

While Hacking Team claims that they do not deal with "repressive regimes,"[89] 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.[90] INSA was already known to be using 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 national security threats.[91]

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 ability to communicate anonymously has become more difficult. The Tor Network anonymizing tool has been blocked since May 2012.

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 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-2015.[92]

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.[93] 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 to monitor user activity themselves.[94]

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 claim that they are consistently threatened by state security agents for their online activism.[95] Prior to their imprisonment in April 2014, the Zone 9 bloggers reported suffering a considerable amount of harassment for their work, leading them to go silent for several months. Shortly after the bloggers announced a resumption of activities on Facebook in April 2014, six Zone 9 bloggers were arrested and sent to a federal detention center in Addis Ababa where they were reportedly mistreated and tortured to give false confessions throughout the year.[96] The active Gmail accounts belonging to several of the Zone 9 bloggers while in detention suggests that they may have been forced give their passwords to security officials against their will.[97]

Ethiopian journalists in the diaspora have also been targeted for harassment, according to one reporter of the diaspora-based website ECADF, who received death threats from an alleged government spy in Netherlands for his reporting.[98]

Technical Attacks

Opposition critics and independent voices face frequent technical attacks, even when based abroad. In recent years, independent research has found evidence that the Ethiopian authorities use sophisticated surveillance malware and spyware, such as FinFisher's FinSpy and Hacking Team's Remote Control Servers (RCS), to target exiled dissidents. The most recent attack was recorded in December 2014 by researchers at Citizen Lab, who discovered RCS spyware in attached documents sent in emails to journalists with the Ethiopian Satellite Television Service (ESAT), an independent TV, radio, and online news outlet run by members of the Ethiopian diaspora in Virginia.[99] Having been targeted with the RCS spyware before,[100] the journalists did not download the attachments that would have installed the spyware and enabled the attackers to access files on the infected computers. The journalists believe the attack was an effort by the authorities to ascertain ESAT's sources within Ethiopia.

Meanwhile, a technical attack in late 2012 and early 2013 on an exiled dissident (and American citizen) is currently the basis of an ongoing legal case at a U.S. District Court filed by the Electronic Frontier Foundation (EFF).[101] In April 2013, EFF sued the Ethiopian government in a U.S. court on behalf of the anonymous Ethiopian dissident for implanting malicious FinSpy malware on the individual's computer. Linked to a server belonging to EthioTelecom, FinSpy had secretly recorded dozens of Skype calls, copied emails the individual had sent, and logged a web search conducted by his son on the history of sports medicine for a school research project. [102]

Notes:

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

[2] Tom Jackson, "Telecoms slow down development of Ethiopian tech scene – iceaddis," humanipo republished on Ethioconstruction, October 22, 2013, http://bit.ly/1ZIzWhw.

[3] International Telecommunication Union, "Percentage of

Individuals Using the Internet, 2000-2014,"http://bit.ly/1cblxxY.
[4] International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2014,"http://bit.ly/1cblxxY.
[5] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2014,"http://bit.ly/1cblxxY.
[6] International Telecommunication Union, "Key ICT data, 2000-2015," http://bit.ly/1cblxxY.
[7] International Telecommunication Union, "Ethiopia Profile (Latest data available: 2013)," ICT-Eye, accessed August 1, 2014, http://bit.ly/1NEnLHk.
[8] Aaron Maasho, "Ethiopia launches 4G mobile service in the capital," ed. Mark Potter, Reuters, March 21, 2015, http://reut.rs/1FP0Pky.
[9] "A short report about Ethio-Telecom recent launch of 4G network in Addis Ababa," EthioTube video, 8:44, April 3, 2015, http://bit.ly/1Ryeb90.
[10] World Bank, "Ethiopia Overview," last updated April 05, 2015,http://www.worldbank.org/en/country/ethiopia/overview.
[11] Ethiopia – Telecoms, Mobile, Broadband and Forecasts, Paul Budde Communication Pty Ltd.:June 2014,http://bit.ly/1ji15Rn.
[12] International Telecommunication Union, "Ethiopia Profile (Latest data available: 2013)."
[13] According to tests by Freedom House consultant in 2015.
[14] Akamai, "Average Connection Speed: Ethiopia," map visualization, The State of the Internet, Q4 (2014),http://akamai.me/1OqvpoS.
[15] Aaron Maasho, "Ethiopia signs $700 mln mobile network deal with China's Huawei," Reuters, July 25, 2013, http://reut.rs/1OpDgVj.
[16] 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, February 3, 2015,http://bit.ly/1OpDvzz.
[17] Jim Cowie, "Syria, Venezuela, Ukraine: Internet Under Fire," Renesys (blog), February 26, 2014,http://bit.ly/1R2z0IT.
[18] Freedom House interviews.
[19] Conducted by Freedom House consultant, March 2015.
[20] Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," Telecentre Magazine, September 2008, http://bit.ly/1ji348h.
[21] "Ethio Telecom to remain monopoly for now," TeleGeography,

June 28, 2013, http://bit.ly/1huyjf7.
[22] Paul Chapman, “New report explores the Ethiopian – telecoms, mobile and broadband – market insights, statistics and forecasts,” WhatTech, May 1, 2015, http://bit.ly/1L46Awu.
[23] “Out of reach,” The Economist, August 24, 2013, http://econ.st/1I1UvJO.
[24] “Out of reach,” The Economist.
[25] 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.
[26] Based on allegations that the Chinese authorities have provided the Ethiopian government with technology that can be used for political repression—such as surveillance cameras and satellite jamming equipment—in the past. See: Addis Neger, “Ethiopia: China Involved in ESAT Jamming,” ECADAF Ethiopian news & Opinion, June 23, 2010, http://bit.ly/1LtSYI9; Gary Sands, “Ethiopia’s Broadband Network – A Chinese Trojan Horse?” Foreign Policy Blogs, Foreign Policy Association, September 6, 2013,http://bit.ly/1FWG8X1.
[27] ENA, “Ericsson to take part in telecom expansion in Ethiopia,” Dire Tube, December 18, 2014,http://bit.ly/1PkZfvA.
[28] The Embassy of the United Stated, “Doing Business in Ethiopia,” http://1.usa.gov/1LtTExh.
[29] World Intellectual Property Organization, “Ethiopia Custom Regulation: No 622/2009,”http://bit.ly/1NveoeB.
[30] Mignote Kassa, “Why Ethiopia’s Software Industry Falters,” Addis Fortune 14, no. 700 (September 29, 2013), http://bit.ly/1VJilWC.
[31] “Proclamation No. 281/2002, Telecommunications (Amendment Proclamation,” Federal Negarit Gazeta No. 28, July 2, 2002, http://bit.ly/1snLgsc.
[32] 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.
[33] Dr. Lishan Adam, “Understanding what is happening in ICT in Ethiopia,” (policy paper, Research ICT Africa, 2012) http://bit.ly/1LDPyJ5.
[34] Halefom Abraha, “THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA,” (paper)http://bit.ly/1huzP0S.
[35] Daniel Berhane, “Ethiopia’s web filtering: advanced technology, hypocritical criticisms, bleeding constitution,” Horns Affairs, January 16, 2011, http://bit.ly/1jTyrH1 .

[36] 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.
[37] Interview with the producer of a website called Mircha.org, http://mircha.org/category/english/ .
[38] Abebe Gelaw, "Exposed: Prof. Constantinos Berhe has two fake degrees," Addis Voice, January 18, 2015,http://bit.ly/1zrOETe.
[39] "BBC condemns Ethiopian broadcast jamming," BBC, May 30, 2014, http://bbc.in/1oCH8VO.
[40] "Ethiopia 'blocks' Al Jazeera aebsites," Al Jazeera, March 18, 2013, http://aje.me/1144wNh.
[41] Zone9, blog post, October 8, 2015, http://zone9ethio.blogspot.com/.
[42] Mohammed Ademo, Twitter post, July 25, 2012, 1:08 p.m.,https://twitter.com/OPride/status/228159700489879552.
[43] Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," Columbia Journalism Review, August 13, 2012, http://bit.ly/1Lm2npk.
[44] Ory Okolloh Mwangi, Twitter post, November 6, 2013, 9:20 a.m.,https://twitter.com/kenyanpundit/status/398077421926514688.
[45] "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.
[46] 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.
[47] 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.
[48] Reporters prevented from reporting on the trial of Zone9 Bloggers: Trial Tracker Blog,http://trialtrackerblog.org/home/ .
[49] 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.
[50] “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.
[51] Chala, “When blogging is held hostage of Ethiopia’s telecom policy.”
[52] “Ethiopia Trains Bloggers to attack its opposition,” ECADF Ethiopian News & Opinions, June 7, 2014,http://bit.ly/1QemZjl.
[53] Markos Lemma, “Disconnected Ethiopian Netizens,” Digital Development Debates (blog),November 2012, http://bit.ly/1MI9Nu3.
[54] “#BBCtrending: Jailed bloggers spark Ethiopia trend,” BBC Trending, April 30, 2014,http://bbc.in/1kpaTDX.
[55] Mahlét Solomon, “Because I am Oromo,” Facebook page for campaign, November 15, 2014,http://on.fb.me/1VJOKag.
[56] Amnesty International, Ethiopia: Because I am Oromo’: Sweeping repression in the Oromia region of Ethiopia, October 28, 2014, http://bit.ly/1QenAS6.
[57] Melody Sundberg, “A 16-Year-Old’s Death Is Forcing Ethiopia to Confront Its Sexual Violence Problem,” Global Voices, January 16, 2015, http://bit.ly/1OqziKr.
[58] Constitution of the Federal Democratic Republic of Ethiopia (1995), art. 26 and 29, accessed, August 24, 2010, http://www.ethiopar.net/constitution.
[59] Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, Federal Negarit Gazeta No. 64, December 4, 2008.
[60] Article 19, The Legal Framework for Freedom of Expression in Ethiopia, accessed September 10, 2014,http://bit.ly/1PI0f33.
[61] Criminal Code, art. 613, http://bit.ly/1OpHE6F.
[62] “A Proclamation on Telecom Fraud Offence,” Federal Negarit Gazeta No. 61, September 4, 2012,http://www.abyssinialaw.com/uploads/761.pdf.
[63] 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.
[64]"Telecommunication Proclamation No. 281/2002, Article 2(11) and 2(12)," Federal Negarit Gazeta No. 28, July 2, 2002, accessed July 25, 2014, http://bit.ly/1jTCWkV. 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).
[65] A Proclamation on Telecom Fraud Offence.
[66] Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences,"legal analysis, August 6, 2012,http://bit.ly/1Lbonjm.
[67] "Anti-Terrorism Proclamation No. 652/2009," Federal Negarit Gazeta No. 57, August 28, 2009.
[68] "EBS Special- The social media boom in Ethiopia," Diretube video, 31:01, February 2015,http://bit.ly/1MIc0FD.
[69] Committee to Protect Journalists,"2014 prison census: 221 journalists jailed worldwide," December 1, 2014, https://cpj.org/imprisoned/2014.php.
[70] "Six members of Zone Nine, group of bloggers and activists are arrested," [in Amharic] Zone9 (blog), April 25, 2014, http://bit.ly/1VJn6ow.
[71]"Federal High Court Lideta Criminal Bench court, Addis Ababa," http://1drv.ms/1OqAjlC.
[72] Endalk Chala, "What You Need to Know About Ethiopia v. Zone9 Bloggers: Verdict Expected July 20," Global Voices Advocacy, July 17, 2015, http://bit.ly/1jTDO9b.
[73] Jared Goyette, "For this group of Ethiopian journalists, the Hacking Team revelations are personal," Public Radio International, July 8, 2015, http://bit.ly/1UN64ID.
[74] "Federal High Court Lideta Criminal Bench court, Addis Ababa."
[75] 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.
[76] Committee to Protect Journalists, "In Ethiopia, Zone 9 bloggers acquitted of terrorism charges," news statement, October 16, 2015, https://www.cpj.org/.../in-ethiopia-zone-9-bloggers-acquitted....
[77] "Defendants in Zelalem Workagegnehu et al Case Reappointed

to December 25th," De Birhan (blog), December 18, 2014, http://bit.ly/1PI0Ph6.
[78] "Ethiopia Charges 10 of Links with Ginbot 7 Movement Today," De Birhan (blog), October 31, 2014,http://bit.ly/1ZIQJRB.
[79] "Ethiopia arrests for young, prominent opposition figures," Ethiomedia, July 8, 2014,http://bit.ly/1MIdQGC.
[80] Tedla D. Tekle, "The Journalism and Scholarship of Attachment – Ethiopia, Africa," Transcend Media Service, May 25, 2015, http://bit.ly/1ZIR46L.
[81]"Court Day of Our Co-Blogger Celalem Workagegnehu et al," De Birhan (blog), March 19, 2015,http://bit.ly/1PI0Vp9; Addis Standard, Facebook post, August 20, 2015, http://on.fb.me/1JXGSWz.
[82] 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.
[83] Human Rights Watch, "They Know Everything We Do," 62.
[84] Human Rights Watch, "They Know Everything We Do," 67.
[85] Ibid, 52.
[86] Committee to Protect Journalists, "Ethiopian Blogger, Journalists Convicted of Terrorism," January 19, 2012, http://cpj.org/x/47b9.
[87] Bill Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, Citizen Lab, March 9, 2015, http://bit.ly/1Ryogmr.
[88] Hacking Team,"Customer Policy," 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://cnet.co/1fo6jJZ.
[90] Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.

[91] Fahmida Y. Rashid, “FinFisher ‘Lawful Interception’ Spyware Found in Ten Countries, Including the U.S.,” Security Week, August 8, 2012, http://bit.ly/1WRPuap.
[92] Interview conducted by Freedom House consultant.
[93] Groum Abate, “Internet Cafes Start Registering Users,” The Capital republished Nazret (blog), December 27, 2006, http://bit.ly/1Lm98aX.
[94] Human Rights Watch, “They Know Everything We Do,” 67.
[95] 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.
[96] Trial Tracker Blog, “Trials.”
[97] Anonymous Freedom House researcher reported seeing several of the detained Zone9 bloggers actively online in Gmail chat.
[98] “ክንፉ አሰፋ በስለላ ከሆላንድ የተባረረው የጋዜጠኛውን አንበት እቆርጣለሁ አለ,” ECADAF Ethiopian News & Opinion, April 12, 2015, http://ecadforum.com/Amharic/archives/14790/ .
[99] Marczak et al., Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.
[100] Bill Marczak, et al., Hacking Team and the Targeting of Ethiopian Journalists, Citizen Lab, February 12, 2014, http://bit.ly/1heE0Nm.
[101] Jenifer Fenton, “Ethiopia spying case casts spotlight on cyber surveillance in US,” Al Jazeera, July 13, 2015, http://alj.am/bhaq.
[102] Electronic Frontier Foundation,“Kidane v. Ethiopia,” last updated August 28, 2014,https://www.eff.org/cases/kidane-v-ethiopia.