Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**227**
Land:	Etiopien
Kilde:	Human Rights Watch
Titel:	"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia
Udgivet:	25. marts 2014
Optaget på baggrundsmaterialet:	22. oktober 2014

HUMAN RIGHTS WATCH

“They Know Everything We Do”

Telecom and Internet Surveillance in Ethiopia

HUMAN RIGHTS WATCH

“They Know Everything We Do”

Telecom and Internet Surveillance in Ethiopia

Printed in the United States of America
ISBN: 978-1-62313-1159
Cover design by Rafael Jimenez

Human Rights Watch is dedicated to protecting the human rights of people around the world. We stand with victims and activists to prevent discrimination, to uphold political freedom, to protect people from inhumane conduct in wartime, and to bring offenders to justice. We investigate and expose human rights violations and hold abusers accountable. We challenge governments and those who hold power to end abusive practices and respect international human rights law. We enlist the public and the international community to support the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amsterdam, Beirut, Berlin, Brussels, Chicago, Geneva, Goma, Johannesburg, London, Los Angeles, Moscow, Nairobi, New York, Paris, San Francisco, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: http://www.Human Rights Watch.org

MARCH 2014 978-1-62313-1159

"They Know Everything We Do"

Telecom and Internet Surveillance in Ethiopia

GLOSSARY OF ABBREVIATIONS

BPR	Business Process Reengineering
CALEA	Communications Assistance for Law Enforcement Act
CESCR	Committee on Economic, Social and Cultural Rights
CITCC	China International Telecom Corporation
CSO Law	Charities and Societies Proclamation
CUD	Coalition for Unity and Democracy
DPI	Deep Packet Inspection
DW	Deutsche Welle
EDF	Ethiopian Defense Forces
EICTDA	Ethiopian Information and Communication Technology Development Agency
EPRDF	Ethiopian People's Revolutionary Democratic Front
EPRP	Ethiopian People's Revolutionary Party
ESAT	Ethiopian Satellite Television
ETA	Ethiopian Telecommunication Agency
ETC	Ethiopia Telecommunications Corporation
GPS	Global Positioning System
ICCPR	International Covenant on Civil and Political Rights
ICS	Intelligent Charging System
ICT	Information and Communications Technology
IM	Instant Message
INSA	Information Network Security Agency
ITU	International Telecommunication Union
MCIT	Ministry of Communications and Information Technology
NGO	Nongovernmental organization
NISS	National Intelligence and Security Services
OLF	Oromo Liberation Front
ONC	Oromo National Congress
ONI	Open Network Initiative
ONLF	Ogaden National Liberation Front
OPC	Oromo People's Congress
PID	Project Information Document

PSCAP	Public Sector Capacity Building Program
SIM	Subscriber Identity Module
SMS	Short Message Service
TPLF	Tigrayan People's Liberation Front
UAV	Unmanned Aerial Vehicles
UDJ	Union for Democracy and Justice
VOA	Voice of America
VOBME	Voice of the Broad Masses of Eritrea
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal
WTO	World Trade Organization
ZTEsec	ZTE Special Equipment Company

Summary

> One day they arrested me and they showed me everything. They showed me a list of all my phone calls and they played a conversation I had with my brother. They arrested me because we talked about politics on the phone. It was the first phone I ever owned, and I thought I could finally talk freely.
> — Former member of an Oromo opposition party, now a refugee in Kenya, May 2013

Since 2010, Ethiopia's information technology capabilities have grown by leaps and bounds. Although Ethiopia still lags well behind many other countries in Africa, mobile phone coverage is increasing and access to email and social media have opened up opportunities for young Ethiopians—especially those living in urban areas—to communicate with each other and share viewpoints and ideas.

The Ethiopian government should consider the spread of Internet and other communications technology an important opportunity. Encouraging the growth of the telecommunications sector is crucial for the country to modernize and achieve its ambitious economic growth targets.

Instead, the ruling Ethiopian People's Revolutionary Democratic Front (EPRDF), a coalition of ethnically-based political parties in power for more than 20 years, continues to severely restrict the rights to freedom of expression, association, and peaceful assembly. It has used repressive laws to decimate civil society organizations and independent media and target individuals with politically-motivated prosecutions. The ethnic Oromo population has been particularly affected, with the ruling party using the fear of the ongoing but limited insurgency by the Oromo Liberation Front (OLF) in the Oromia region to justify widespread repression of the ethnic Oromo population. Associations with other banned groups, including Ginbot 7, are also used to justify repression.

As a result, the increasing technological ability of Ethiopians to communicate, express their views, and organize is viewed less as a social benefit and more as a political threat

for the ruling party, which depends upon invasive monitoring and surveillance to maintain control of its population.

The Ethiopian government has maintained strict control over Internet and mobile technologies so it can monitor their use and limit the type of information that is being communicated and accessed. Unlike most other African countries, Ethiopia has a complete monopoly over its rapidly growing telecommunications sector through the state-owned operator, Ethio Telecom. This monopoly ensures that Ethiopia can effectively limit access to information and curtail freedoms of expression and association without any oversight since independent legislative or judicial mechanisms that would ensure that surveillance capabilities are not misused do not exist in Ethiopia.

All governments around the world engage in surveillance, but in most countries at least some judicial and legislative mechanisms are in place to protect privacy and other rights. In Ethiopia these mechanisms are largely absent. The government's actual control is exacerbated by the perception among Ethiopia's population that government surveillance is omnipresent. This results in considerable self-censorship, with many Ethiopians refraining from openly communicating on a variety of topics across the telecom network.

This report is based on research conducted between September 2012 and February 2014, including interviews with more than 100 people in 11 countries. It documents how the Ethiopian government uses its control over the telecommunications system to restrict the right to privacy and freedoms of expression and association, and access to information, among other rights. These rights are entrenched in international law and frequently touted by the government as part of Ethiopia's constitution. In practice, they are undercut by problematic national laws and practices by the authorities that wholly disregard any legal protections.

Websites of opposition parties, independent media sites, blogs, and several international media outlets are routinely blocked by government censors. Radio and television stations are routinely jammed. Bloggers and Facebook users face harassment and the threat of arrest should they refuse to tone down their online writings. The message is simple: self-censor to limit criticism of the government or you will be censored and subject to arrest.

Information gleaned from telecom and Internet sources is regularly used against Ethiopians arrested for alleged anti-government activities. During interrogations, police show suspects lists of phone calls and are questioned about the identity of callers, particularly foreign callers. They play recorded phone conversations with friends and family members. The information is routinely obtained without judicial warrants. While this electronic "evidence" appears to be used mostly to compel suspects to confess or to provide information, some recorded emails and phone calls have been submitted as evidence in trials under the repressive Anti-Terrorism Proclamation.

The government has also used its telecom and Internet monopoly to curtail lawful opposition activities. Phone networks have been shut down during peaceful protests. Some high-profile Ethiopians in the diaspora have been targeted with highly advanced surveillance tools designed to covertly monitor online activity and steal passwords and files.

In rural Ethiopia, where phone coverage and Internet access is very limited, the government maintains control through extensive networks of informants and a grassroots system of surveillance. This rural legacy means that ordinary Ethiopians commonly view mobile phones and other new communications technologies as just another tool to monitor them. As a result, self-censorship in phone and email communication is rampant as people extend their long-held fears of government interference in their private lives to their mobile phone use. These perceptions of phone surveillance are far more intrusive than the reality, at least at present.

Ethiopia has acquired some of the world's most advanced surveillance technologies, but the scale of its actual telecom surveillance is limited by human capacity issues and a lack of trust among key government departments. But while use of these technologies has been limited to date, the historic fear of ordinary Ethiopians of questioning their government and the perception of pervasive surveillance serves the same purpose: it silences independent voices and limits freedom of speech and opinion. Human Rights Watch research suggests that this may just be the beginning: Ethiopians may increasingly experience far more prevalent unlawful use of phone and email surveillance should the government's human capacity increase.

While monitoring of communications can legitimately be used to combat criminal activity, corruption, and terrorism, in Ethiopia there is little in the way of guidelines or directives on

surveillance of communications or use of collected information to ensure such practices are not illegal. In different parts of the world, the rapid growth of information and communications technology has provided new opportunities for individuals to communicate in a manner and at a pace like never before, increasing the space for political discourse and facilitating access to information. However, many Ethiopians have not been able to enjoy these opportunities. Instead, information and communications technology is being used as yet another method through which the government seeks to exercise complete control over the population, stifling the rights to freedom of expression and association, eroding privacy, and limiting access to information—all of which limit opportunities for expressing contrary opinions and engaging in meaningful debate.

Court warrants are required for surveillance or searches but in practice none are issued. Intercepted communications have become tools used to crack down on political dissenters and other critics of the ruling party. Opposition party members, journalists, and young, educated Oromos are among the key targets.

The infrastructure for surveillance was not created by the Ethiopian government alone, but with the support of investors in the Internet and telecom sector, including Chinese and European companies. These foreign companies have provided the products, services, and expertise to modernize the sector.

Ethiopia should not only ensure that an appropriate legal framework is in place to protect and respect privacy rights entrenched in international law, but also that this legal framework is applied in practice. Companies that provide surveillance technology, software, or services should adopt policies to ensure these products are being used for legitimate law enforcement purposes and not to repress opposition parties, journalists, bloggers, and others.

Recommendations

To the Government of Ethiopia

- Enact protections for the right to privacy to prevent abuse and arbitrary use of surveillance, national security, and law enforcement powers as guaranteed under international law applicable to Ethiopia. Surveillance should occur only as provided in law, be necessary and proportionate to achieve a legitimate aim, and be subject to both judicial and parliamentary oversight.
- Legal safeguards should limit the nature, scope, and duration of possible surveillance, the grounds required for ordering them, and the authorities competent to authorize, carry out, and supervise them.
- Ensure that information obtained through email or telephone interception or access to call records is inadmissible in courts unless a court warrant has been obtained. All laws enabling the admissibility of intercepted information in court should be amended to require a court warrant, including the Criminal Code, the Telecom Fraud Proclamation, and the Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation.
- Enact protections for call records and other "metadata" so that such information may not be collected or accessed by police, security, or intelligence agencies without a court order and oversight to prevent abuse, unauthorized use or disclosure of that information.
- Enforce the requirements for a court warrant prior to interception/surveillance under the Anti-Terrorism Proclamation and the NISS Proclamation. Ethio Telecom should not provide access to metadata or recorded phone calls without a warrant from a competent, independent and impartial court in line with international standards. Any data collection or surveillance conducted by the Information Network Security Agency (INSA) or National Intelligence and Security Services (NISS) should require prior court approval.
- Immediately unblock all websites of political parties, media, and bloggers and commit to not block such websites in the future.
- Immediately cease all jamming of radio and television stations and commit to not jam radio and television stations in the future.
- Cease harassing individuals for exercising their right to freedom of expression online through social media and blogs.

- Appropriately discipline or prosecute officials, regardless of rank or position, who arbitrarily arrest or detain or ill-treat individuals on the basis of unlawfully intercepted or acquired information. Impose criminal penalties for illegal surveillance by public or private actors.
- Report annually on the government's use of surveillance powers. This reporting should include: the number of data requests made to Ethio Telecom, cybercafés, or other mobile and Internet service providers; the number of requests for real-time interception or recording of phone calls; and the number of individuals or accounts that were implicated by such requests.
- Provide protections for the rights to freedom of expression and privacy to prevent abuse of emergency powers to shut down networks or intercept communications.
- Repeal or amend all laws that infringe upon privacy rights, the right to information, and the rights to freedom of expression, association, movement, and peaceful assembly, including the Anti-Terrorism Proclamation, the NISS Proclamation, the Telecom Fraud Proclamation, and the Prevention and Suppression of Money Laundering and the Financing of Terrorism, to bring them in line with international standards. Amendments should include the following articles:
    - Anti-Terrorism Proclamation, article 23(1) and (2) (permitting non-disclosure of information sources and hearsay) and the NISS Proclamation, article 27 (requiring cooperation with NISS information requests). Ethio Telecom and INSA officials should cooperate with NISS only when a court warrant is granted facilitating access to user information.
    - Telecom Fraud Proclamation, articles 6(1) (criminalizes dissemination of messages about activities punishable under the anti-terrorism law) and 10(3) (criminalizes commercial use of VoIP).

To International Technology and Telecom Companies Serving Ethiopia

- Assess human rights risks raised by potential business activity, including risk posed to the rights of freedom of expression, access to information, association, and privacy. Assessments should address risk of misuse of non-customized, "off-the-shelf" equipment sold to governments that may be used to facilitate illegal surveillance or censorship. Assessments should also address the risk of customizing products and services for law enforcement, intelligence, and security agency customers.
- As part of a tender or contract negotiation process, inquire about the end use and end users of the products or services being provided, especially for "dual use" products, including "lawful intercept" surveillance software and equipment.

- Develop strategies to mitigate the risk of abuses linked to business operations and new contracts, including by incorporating human rights safeguards into business agreements. Such strategies should be consistent with the Global Network Initiative (GNI) principles and the United Nations "Protect, Respect, and Remedy" Framework for business and human rights.
- Adopt policies and procedures to stop or address misuse of products and services, including contractual provisions that designate end use and end users, the violation of which would allow the company to withdraw services or cease technical support or upgrades. Promptly investigate any misuse of products or services and take concrete steps to address human rights abuses linked to business operations.
- Adopt human rights policies outlining how the company will resist government requests for censorship, illegal surveillance, or network shutdowns, including procedures for narrowing requests that may be disproportionate or challenge requests not supported by law.
- Extend human rights policies and procedures to address the actions of resellers, distributors, and other business partners.
- Commit to independent and transparent third-party monitoring to ensure compliance with human rights standards, including by joining a multi-stakeholder initiative like the GNI.
- Advocate for reform of surveillance or censorship laws to bring them in line with international human rights standards.
- Review any contracts or engagements initiated before 2008 and craft strategies to address and mitigate any adverse harm that may flow from operations that currently continue under these contracts, consistent with guidance provided by the GNI and UN principles, both launched in 2008. As contracts come up for renewal, incorporate human rights safeguards into newly negotiated contracts.

To the Governments of China, Germany, Italy, the United Kingdom, and Others

- Regulate the export and trade of "dual use" surveillance and censorship technologies such as deep packet inspection equipment and intrusion software. Require such companies subject to national jurisdiction operating abroad to report on any human rights policies and due diligence activity to prevent rights abuses and remedy them if they arise.
- Introduce or implement legal frameworks, such as an independent ombudsperson, that allow government institutions to monitor the human rights performance of companies selling surveillance software, technology, or services subject to national

jurisdiction when they operate abroad in areas that carry serious human rights risks. Frameworks should include an effective complaints mechanism accessible to individuals and communities in Ethiopia, and those representing them, who allege harmful conduct or impact by companies subject to national jurisdiction doing business in Ethiopia, with findings and decisions binding on companies.

- Communicate an expectation to the government of Ethiopia that companies operating in Ethiopia should be able to implement the recommendations outlined above.

To the World Bank, African Development Bank, and other Donors

- Undertake human rights due diligence on telecommunication projects in Ethiopia, to prevent directly or indirectly supporting violations of the rights to privacy or freedom of expression, association, or movement; or access to information including through censorship, illegal surveillance, or network shutdowns. This should include assessing the human rights risks of each activity prior to project approval and throughout the life of the project, identifying measures to avoid or mitigate risks, and comprehensively supervising the projects including through third parties. This due diligence should extend to any government or private sector partners to ensure that they are not implicated in violations.
- Publicly and privately raise with government officials concerns about censorship, illegal surveillance, and network shutdowns and that human rights violations may undermine development priorities.

Methodology

This report is based on research conducted between September 2012 and February 2014 in Ethiopia and 10 other countries, including interviews with Ethiopians living outside the country. The report documents through interviews, review of secondary material, and Internet filtering testing, how the Ethiopian government uses its control over the telecommunications system to restrict the right to privacy and freedoms of expression, information, and association, among other rights.

Over 100 individuals were interviewed, including those whose right to privacy, access to information, and freedom of expression have been abused, former and current intelligence and security officials, Ethio Telecom employees, and other government officials. All were interviewed individually. Interviews were carried out in person and via telephone in Ethiopia, Kenya, Uganda, South Sudan, Israel, the United States, and five countries in Europe.[1] Interviewees included people from a wide range of backgrounds, age, ethnicity, urban, rural, and geographic origin.

Interviews were all conducted in English or with interpreters from Amharic, Afan Oromo, or other Ethiopian local languages into English. Different interpreters were used. Human Rights Watch took various precautions to verify the credibility of interviewees' statements. None of the interviewees were offered any form of compensation for agreeing to participate in interviews. All interviewees voluntarily consented to be interviewed and were informed of the purpose of the interview and its voluntary nature, including their right to stop the interview at any point.

In addition to interviews, Human Rights Watch consulted a variety of secondary material, including academic articles and NGO reports, that corroborates details or patterns described in the report. This material includes previous Human Rights Watch research as well as information collected by other credible technology experts and independent human rights investigators.

[1] United Kingdom, Germany, Norway, Sweden, and Belgium.

Internet filtering testing was carried out in Ethiopia in July and August 2013 in collaboration with the University of Toronto's Citizen Lab, an institute that conducts research on information technology, human rights, and global security. Testing was carried out in Addis Ababa and several other cities. Human Rights Watch tested whether Uniform Resource Locators (URLs) were accessible within the country, with a focus on those websites that had a reasonable likelihood of being blocked based on the Open Network Initiative's (ONI) previous testing in 2012. ONI's 2012 investigation also tested whether a range of websites were accessible from within Ethiopia. For this report, a total of 19 tests were run over seven different days to ensure reliability of results.

In part because the Ethiopian government restricts human rights research in the country, this report is not a comprehensive assessment of the surveillance situation in Ethiopia. Human Rights Watch and other independent national and international human rights organizations face extraordinary challenges to carrying out investigations in Ethiopia. This is mainly because of the difficulty of assuring the safety and confidentiality of victims of human rights abuses, given the government's hostility towards human rights investigation and reporting. Increasingly, the families of individuals outside of Ethiopia who provide information can also be at risk of reprisals.

The Ethiopian government routinely dismisses Human Rights Watch reports, regularly criticizes Human Rights Watch as an organization, and dismisses the findings of our research. This heightens concerns that any form of involvement with Human Rights Watch, including speaking to the organization, could be used against individuals. The authorities have, in the past, harassed and detained individuals for providing information to, or meeting with, international human rights investigators and journalists.

Human Rights Watch conducted research for this report inside Ethiopia, but many of the people were interviewed outside of the country, making it easier for them to speak openly about their experiences. For fear of possible reprisals, all names and identifying information of interviewees have been removed, and locations of interviews withheld, where such information could suggest someone's identity. In certain cases, pertinent information has been omitted altogether because of concerns that disclosing such information would reveal the identity of interviewees.

Human Rights Watch wrote to the government of Ethiopia, ZTE, Sinovatio (previously known as ZTE Special Equipment Company), Huawei, France Telecom-Orange, Hacking Team, Gamma/FinFisher, and the World Bank to request input on the findings from this report.[2] Any responses received were included in this report as annexes or posted on the Human Rights Watch website.

[2] ZTE and Huawei are based in China. Gamma/FinFisher are based in Germany and the UK. Hacking Team is incorporated in Italy.

I. Background

Patterns of Repression and Government Control

Since the Ethiopian People's Revolutionary Democratic Front (EPRDF) came to power in 1991, a coalition of ethnically-based political parties led by the Tigrayan People's Liberation Front (TPLF), has used various means to consolidate political power.[3]

Repressive measures aimed at restricting freedom of expression and association, as well as access to information, have increased since the controversial 2005 elections.[4] These measures include the harassment, arbitrary detention, and prosecution of opposition leaders, journalists, and activists. The passage in 2009 of the Anti-Terrorism Proclamation (anti-terrorism law) and the Charities and Societies Proclamation (CSO law) further stifled critical voices. The anti-terrorism law has been used to charge and convict journalists, religious leaders, and others for exercising their rights to free expression and peaceful assembly. Many nongovernmental organizations that worked on human rights, governance, and other issues affected by the CSO law have been forced to close or curtail their activities. Little dissent is allowed and individuals are frequently detained for openly questioning government policies and perspectives.[5]

Independent media in Ethiopia has also been decimated in recent years. Very few independent publications exist, and the continual threat of being charged under the anti-terrorism law hangs over journalists who are critical of the government.[6] Many journalists opt for self-censorship instead, avoiding topics deemed politically sensitive. Directives

---

[3] Human Rights Watch, *"One Hundred Ways of Putting Pressure": Violations of Freedom of Expression and Association in Ethiopia*, March 24, 2010, http://www.hrw.org/reports/2010/03/24/one-hundred-ways-putting-pressure-0.

[4] The 2005 elections were marred by serious voting irregularities and a lack of transparency in an election strongly criticized by independent observers. The violent period that followed the 2005 elections resulted in hundreds of deaths, an estimated 30,000 arrests, and charges for treason for many of the opposition leaders. For an overview of the issues surrounding the 2005 election, see Human Rights Watch, *"One Hundred Ways of Putting Pressure"*.

[5] See Human Rights Watch's 2014 World Report chapter on Ethiopia, which provides an overview of Ethiopia's human rights record. Human Rights Watch, *World Report 2014* (New York: Human Rights Watch, 2014), Ethiopia chapter, http://www.hrw.org/world-report/2014/country-chapters/ethiopia.

[6] Only Somalia and Iran have seen more journalists flee their country than Ethiopia between June 2012 and May 2013. Committee to Protect Journalists, "55 Journalists Forced Into Exile June 1, 2012-May 31, 2013," 2013, http://www.cpj.org/exile/2012-2013.php (accessed October 28, 2013).

have been passed making printing presses liable for the content of their publications and radio and television stations are either state-run or minimize criticisms of government policy in order to be able to operate.[7]

Ethiopia's ruling party also dominates the political, economic, and social spheres by completely controlling access to state resources, employment, and benefits.[8] This dual strategy of restricting independent voices and encouraging ruling party support paid off for the ruling party in the 2010 parliamentary elections, as the EPRDF won 99.6 percent of the seats, although this raised many questions about the conduct of the elections.[9]

One reason for the EPRDF's political dominance is that it implements an effective and pervasive community-level surveillance system throughout Ethiopia, a system that relies on active monitoring and reporting of various kinds of activity. But it also benefits from deeply entrenched historical and social attitudes towards the government. The EPRDF uses its well-established network of informants throughout the country to monitor the activities and movements of individuals and households at the *kebele* (village) level, often intimidating them into supporting the ruling party. A complex system of individual and household surveillance is in place. Commonly known as the 5:1 system, it has many variations depending on location but all involve Ethiopians monitoring the day-to-day activities of other Ethiopians, including friends, family members, colleagues, and neighbors.[10] Information on a stranger visiting a rural village or individuals who are openly soliciting support for opposition political parties, for example, are usually swiftly reported to *kebele* leaders. Dissenters are dealt with in a variety of ways, from informal pressure to threats. Continued dissent is passed up the chain of command for further action. In most cases, the mere knowledge that someone may be monitoring your activities is enough to restrict free speech and compel you to self-censor.

Strategically-placed individuals—teachers and police officers, for instance—have increased monitoring responsibilities. These surveillance systems are set up throughout

---

[7] Committee to Protect Journalists, "55 Journalists Forced Into Exile June 1, 2012-May 31, 2013," 2013, http://www.cpj.org/exile/2012-2013.php (accessed October 28, 2013).

[8] Human Rights Watch, *Development Without Freedom: How Aid Underwrites Repression in Ethiopia*, October 19, 2010, http://www.hrw.org/reports/2010/10/19/development-without-freedom-0.

[9] See Human Rights Watch, *World Report 2011* (New York: Human Rights Watch, 2011), Ethiopia chapter, http://www.hrw.org/world-report-2011/world-report-2011-ethiopia.

[10] Human Rights Watch, "*One Hundred Ways of Putting Pressure"* and Human rights Watch interview #91 (name withheld), Kenya, July 2013.

the country to monitor election compliance, to gather intelligence, and to serve other functions. Since anybody could be an informant, the net effect is that people are very afraid to speak openly to anyone but their closest confidants. There is very little in the way of public discourse about sensitive political issues and little opportunity to express dissent in a safe manner.

Ethiopia's population remains predominantly rural, over 85 percent, and these tools and techniques of repression are effective in a country where phone use is still limited and much communication remains by word of mouth.[11] But recent years have seen a rapid increase of mobile phone and Internet use throughout the country. Ethiopia has ambitious growth plans in its telecommunications sector and a reliable and widespread telecom service is crucial for the government to reach its economic targets.[12] Telecommunications growth will give Ethiopians new and unprecedented opportunities to share news, ideas, and access information in a timely manner. However, these developments also present a challenge for government: how to embrace the many economic benefits of a growing telecom sector while ensuring that increased access does not translate into unfettered social and political mobilization and public protest of the kind seen in North Africa and the Middle East in recent years.

Targets of Surveillance

While the Ethiopian government has legitimate national security concerns, government's use of surveillance puts a significant focus on individuals deemed to be a political, rather than a security, threat.

According to former intelligence officials who spoke to Human Rights Watch, the selection of some surveillance targets is not necessarily based on the security threat they pose, and the actual methods of surveillance are sometimes unlawful. More intensive surveillance is undertaken on individuals who are connected with opposition parties—whether registered political parties or those that the government has listed as criminal or terrorist organizations. Individuals who speak to journalists or opposition figures are also often

[11] Human Rights Watch, *"One Hundred Ways of Putting Pressure"* and Human Rights Watch interviews (name withheld), Kenya, July and August 2013.

[12] Federal Democratic Republic of Ethiopia, "Growth and Transformation Plan," 2010.

targeted, and in the past few years those associated with the Muslim protests have come under increased monitoring.[13]

Former intelligence officials told Human Rights Watch that prominent individuals suspected of being connected with opposition political parties and armed movements, especially Ginbot 7 and the Oromo Liberation Front (OLF), are frequently the focus of targeted telecom surveillance. Intelligence officials also said that officials from registered political parties including the Union for Democracy and Justice (UDJ) are also frequent targets of surveillance.[14] The security services may also target individuals due to their ethnicity or family connections, irrespective of whether they belong to a banned organization.

The Ethiopian government considers Ginbot 7, the OLF, and the Ogaden National Liberation Front (ONLF) to be terrorist organizations under the Anti-Terrorism Proclamation.[15] Ginbot 7 was formed by some former members of the opposition Coalition for Unity and Democracy (CUD) party who fled Ethiopia after being detained and convicted of "outrages against the constitution," among other charges, following the controversial 2005 elections.[16] Ginbot 7 is based outside of Ethiopia, has not contested any of Ethiopia's elections, and some of its leaders have been convicted under various laws. It is not a legally registered political party.

The Oromo Liberation Front (OLF) is one of the oldest ethnic Oromo political organizations, founded in the 1960s as part of Oromo nationalist movements fighting against the Haile

---

[13] Since 2012, Ethiopia has seen large-scale public demonstrations by parts of its Muslim community, which constitutes about a third of the country's population. The protests stem from the Ethiopian government's alleged interference in religious affairs. The protests have been met with excessive force from security forces and many have been detained and charged under the anti-terrorism law. See Human Rights Watch, *World Report 2013* (New York: Human Rights Watch, 2013), Ethiopia chapter, http://www.hrw.org/world-report/2013/country-chapters/ethiopia and "Prominent Muslims Detained in Crackdown," Human Rights Watch news release, August 15, 2012, http://www.hrw.org/news/2012/08/15/ethiopia-prominent-muslims-detained-crackdown.

[14] Human Rights Watch interview with former government employee # 8, (location withheld), January 2013.

[15] Article 25 of the Anti-Terrorism Proclamation enables Ethiopia to designate terrorist organizations. Currently Ginbot 7, OLF, ONLF, al-Shabaab, and al-Qaeda have been designated. Committee to Protect Journalists, "In Ethiopia, anti-terrorism law chills reporting on security," June 24, 2011, http://www.cpj.org/blog/2011/06/in-ethiopia-anti-terrorism-law-chills-reporting-on.php (accessed November 26, 2013).

[16] Amnesty International, "Justice under fire: Trials of opposition leaders, journalists, and human rights defenders in Ethiopia," July 2011, http://www.amnesty.org/en/library/info/AFR25/002/2011/en (accessed March 14, 2014). See Human Rights Watch, *"One Hundred Ways of Putting Pressure"* for more information on the controversial 2005 elections.

Selassie government.[17] The OLF's fragile alliance with the TPLF splintered early in the 1990s and it withdrew from elections and government. Since then it has waged what most observers view as a fairly limited and ineffectual armed resistance against the EPRDF.[18] However, the government uses the specter of an ongoing OLF "armed struggle" to justify widespread repression of Oromo individuals. Regional government and security officials routinely accuse dissidents, critics and students of being OLF "terrorists" or insurgents. Thousands of Oromo from all walks of life have been targeted for arbitrary detention, torture and other abuses even when there has been no evidence linking them to the OLF.[19]

Human Rights Watch interviews suggest that a significant number of Oromo individuals have been targeted for unlawful surveillance. Those arrested are invariably accused of being members or supporters of the OLF. In some cases, security officials may have a reasonable suspicion of these individuals being involved with OLF. But in the majority of cases, Oromos were under surveillance because they were organizing cultural associations or trade unions, were involved in celebrating Oromo culture (through music, art, etc.) or were involved in registered political parties.

Like the OLF, the Ogaden National Liberation Front (ONLF) was initially a political party, but began a low-level armed insurgency in Ethiopia's Somali region in response to what it perceived to be the EPRDF's failure to respect regional autonomy, and to consider demands for self-determination.[20] In 2007, the ONLF scaled up armed attacks against government targets and oil exploration sites, triggering a harsh crackdown by the government.[21] As with the government's counterinsurgency response to the OLF, the Ethiopian security forces have routinely committed abuses against individuals of Somali ethnicity, including arbitrary detentions, torture, and extrajudicial killings, based on their ethnicity or perceived support for the ONLF.

---

[17] Human Rights Watch, *Suppressing Dissent: Human Rights Abuses and Political Repression in Ethiopia's Oromia Region,* Vol. 17, No. 7 (A), May 10, 2005, http://www.hrw.org/reports/2005/05/09/suppressing-dissent-0.

[18] Ibid.

[19] Ibid.

[20] Human Rights Watch, *Collective Punishment: War Crimes and Crimes against Humanity in the Ogaden area of Ethiopia's Somali Regional State*, June 13, 2008, http://www.hrw.org/reports/2008/06/12/collective-punishment; and International Crisis Group, "Ethiopia: Prospects for Peace in the Ogaden," August 2013, http://www.crisisgroup.org/~/media/Files/africa/horn-of-africa/ethiopia-eritrea/207-ethiopia-prospects-for-peace-in-ogaden.pdf (accessed February 12, 2014).

[21] Human Rights Watch, *Collective Punishment*.

Since the passage of the Anti-Terrorism Proclamation in 2009, Ethiopia has used its overly broad provisions to target individuals and organizations that express opinions contrary to government policy or positions, often claiming that they are members or supporters of these banned organizations. While the government may have legitimate security interests in monitoring individuals who support armed anti-government movements, there are two serious concerns with the manner in which the authorities conduct surveillance activities. One is that even where an individual may be a legitimate target, the methods used to monitor and investigate their activities can be unlawful, for instance disregarding the need for judicial warrants. A second concern is that the Ethiopian security forces have repeatedly targeted a broad spectrum of individuals based solely on ethnicity, participation in lawful activities, or family connections. One former intelligence official said:

> We would often try to gather specific evidence that people were linked to terrorist groups like OLF, ONLF, or Ginbot 7. Ginbot 7 [is] not a problem in the country anymore, and they know that but they are still using the threat of Ginbot 7 to harass people, even if there is no threat. OLF is not a terrorist threat either. ONLF is the only real threat. Oromo people, especially the young, still have sentiment for OLF. They [the authorities] use OLF to marginalize Oromos—there is a threat from the idea of OLF, but not from the actual OLF.[22]

Former intelligence officials also described the gathering of intelligence on international NGOs. Information was often collected about the individuals employed, the finances of the organization, and the NGO's foreign connections.[23] It is not known how widespread NGO surveillance is in Ethiopia. Most of the intelligence was gathered from individuals employed by the organization who were acting as informants or from intelligence officials who were hired as employees in some other capacity in the organization. Use of telephone or email surveillance was minimal according to former intelligence officials. However, one former intelligence official involved in the monitoring of several foreign NGOs told Human Rights Watch that, "We have the potential and there is nothing to stop us from doing

[22] Human Rights Watch interview with former government employee # 8, (location withheld), January 2013.
[23] Human Rights Watch interview with former government employee # 22, (location withheld), April 2013.

that."[24] The Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation 657/2009 gives security officials broad powers of surveillance over the financial activities of NGOs.[25]

Former officials also described to Human Rights Watch being involved in gathering intelligence on Ethiopians living in the diaspora. This involved "old-school" techniques of infiltrating diaspora communities and gathering information on the key diaspora players and the extent of their involvement in Ethiopian politics or media. There is no evidence that emails or telephone calls are monitored in any substantive way. There are increasing reports of Ethiopian embassies in various capitals putting more and more effort into recruiting informants within diaspora communities. Former government officials report that the government facilitates individuals acquiring scholarships to study abroad in order to recruit those individuals as informants. Ministry of Foreign Affairs officials play a significant role in this and, according to several former employees, maintain records of financial transactions from the diaspora to Ethiopians in-country. Ostensibly this is part of Ethiopia's efforts to combat the financing of terrorism and money laundering but information is kept that goes far beyond that.[26]

With a young population, many Ethiopians know nothing other than extensive government control over their lives, and it is through this lens that many view the opportunities that enhanced access to mobile and Internet services may bring to their lives. A refugee currently living in Kenya summed up the situation:

> They have complete control. I was a teacher and was told I needed to join [EPRDF], I refused and was fired. My family [members] were farmers, because of me they did not receive seeds or any benefits from the *kebele*. "That is for government" they were told. Everyone I know is angry with our government, but people are fearful for their lives if they get involved in politics. There are thousands of people here in [refugee location] who have

[24] Human Rights Watch interview with former government employee # 8, (location withheld), January 2013.

[25] Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation 657/2009, art. 12, 25.

[26] Human Rights Watch interview with former government employee # 23, (location withheld), April 2013 and Human Rights Watch interview with former government employee #30, (location withheld), May 2013. The Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation 657/2009 contains overly broad provisions granting surveillance powers over a wide variety of individuals and organizations.

> fled because they dared question government. Mobile phones came to my *kebele* [village] several years ago. At first we were excited but it hasn't made any difference to us, it's just another way they control us. They listen to our calls and arrest us if we talk to people they don't like. All this so-called development hasn't changed anything—they still have complete control, we can't say anything, we are still poor, and if you don't support their ways you end up living here [as a refugee].[27]

The opportunities that these technologies provide to increase freedoms of expression, access to information, and freedom of association are greatly diminished for those living in fear as they are afraid to use these technologies to their full extent. As one man said, "We have no choice in the matter. They run the phone service. They know our phone number and where we live. They know everything about us."[28]

Fears of Surveillance

Many Ethiopians believe that the introduction of technologies such as the mobile phone and Internet-based technologies are a new way for the government to exercise control and monitor Ethiopians. Such perceptions may derive in part from Ethiopia's long history of highly authoritarian and centralized governance, which stretches back well before the EPRDF.[29]

Many Ethiopians with whom Human Rights Watch spoke thought that all their phone calls and emails are monitored, and that none of these mediums are safe to communicate on. Because of the perception and fear of surveillance, they said they self-censor their telephone and Internet communications. These fears appear to persist to different degrees throughout the country, regardless of ethnicity. Many told Human Rights Watch that the basis for their fear was rumors of arrests due to the contents of phone calls but very few people could provide specific details. Even more described hearing of others being arrested based on receiving phone calls from certain people outside of Ethiopia.

---

[27] Human Rights Watch interview #99 (name withheld), Kenya, July 2013.

[28] Human Rights Watch interview #31 (name withheld), Kenya, May 2013.

[29] Human Rights Watch/Africa Watch, *Evil Days: Thirty Years of War and Famine in Ethiopia* (New York: Human Rights Watch, September 1991), http://www.hrw.org/sites/default/files/reports/Ethiopia919.pdf.

Many refugees who have fled Ethiopia for various reasons told Human Rights Watch they have been told by their relatives in Ethiopia not to call because it is too dangerous. Inside Ethiopia, many individuals avoid communicating about many topics, or only answer in very innocuous ways or speak using a variety of code words. As one man said, "We use so many code words and avoid talking directly about so many topics that often I'm not sure I know what we are really talking about."[30] Other individuals stated that the phone is only used to make appointments with no substantive conversation ever taking place. The net effect is that the fear of telephone surveillance adds to the harms caused by the reality of phone surveillance—it restricts what people are willing to communicate and with whom they are willing to communicate.

Self-censorship is also prevalent in email and online communications. Very few people who spoke to Human Rights Watch, including senior government officials, ever use their .et email addresses because of the perception of pervasive surveillance. Many individuals within Ethiopia use fake email addresses and avoid using certain sensitive keywords. Others refuse to use email altogether. One notable exception to this is Facebook, where Ethiopians seem to speak much more openly.[31]

Regional and *woreda*-level government employees also practice high degrees of self-censorship and many will not communicate about sensitive subjects on email or telephone. NGO workers and foreign government officials also readily censor the contents of their messages, unclear about the actual extent of surveillance and not willing to risk reprisals.

As a former farmer from Oromia told Human Rights Watch:

> We all know they watch every step we make. We can't go anywhere without them knowing, we can't speak bad things about government without having trouble, we can't get education or services without supporting them. We know they listen to all our phone calls and Internet. We know all of this, but what can we do? We are all too scared to speak our mind.[32]

[30] Human Rights Watch interview #33 (name and location withheld), May 2013.

[31] It is unclear why Facebook is an exception although one blogger told Human Rights Watch it was because Facebook is a relatively new technology in Ethiopia and individuals have the perception that their postings are anonymous.

[32] Human Rights Watch interview #48 (name withheld), Kenya, May 2013.

Telecommunications and Media in Ethiopia

Mobile phone usage has grown dramatically in Ethiopia in the last few years, although coverage is still very limited in comparison to other sub-Saharan African countries. According to the International Telecommunication Union (ITU), Ethiopia has 23.7 users per 100 people and just 0.9 landline subscribers per 100 people.[33] By way of comparison, neighboring Kenya has 72 mobile subscriptions per 100 people and Nigeria has 68 mobile subscriptions per 100 people.[34] Mobile rates are expensive and the network is prone to frequent and lengthy outages, particularly outside of Addis Ababa, much to the frustration of Ethiopians.[35] While mobile phone use is increasing, many Ethiopians in more remote areas continue to rely either on shared landlines or on VSAT telephones available at the local Ethio Telecom office.[36]

The majority of Internet sites with Ethiopian content are hosted on servers outside of Ethiopia and are run by the diaspora, although the number of websites hosted by Ethiopians in-country are increasing. Many Ethiopian sites are in English, although there are a significant and increasing number of Amharic sites available along with a number of sites in Somali and Afan Oromo.

Internet usage in Ethiopia is still in its infancy with less than 1.5 percent of Ethiopians connected to the Internet and fewer than 27,000 broadband subscribers countrywide. By contrast, neighboring Kenya has close to 40 percent access.[37] The majority of Internet users

---

33 The International Telecommunication Union (ITU) is a specialized agency of the United Nations tasked with promoting technical interoperability of telecommunications networks. They "allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide." International Telecommunication Union (ITU), "Overview," 2014, http://www.itu.int/en/about/Pages/overview.aspx (accessed February 12, 2014). Data from ITU's Ethiopia country profile is available at: ITU, "ITU Regional Office for Africa, Ethiopia," 2014, http://www.itu.int/ITU-D/afr/memberstates/country_details.asp?countryIndex=ETH (accessed February 12, 2014).

34 ITU, "Measuring the information Society," 2012, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf (accessed March 14, 2014).

35 Yonas Abiye, "MPs lambast Debretsion over Ethio-telecom's 'poor service,'" *The Reporter,* May 18, 2013, http://www.thereporterethiopia.com/index.php/news-headlines/item/500-mps-lambast-debretsion-over-ethio-telecom%E2%80%99s-%E2%80%9Cpoor-service%E2%80%9D (accessed September 30 2013).

36 Very Small Aperture Terminal (VSAT) is a satellite-based telephone service that is used to connect small remote areas to the Ethio Telecom infrastructure without the need of physical connection to the infrastructure. Ethiopians can use phones connected by Ethio Telecom offices in remote areas. As mobile coverage increases across Ethiopia, VSAT is being phased out.

37 According to Internet World Stats, as of December 31, 2012, there were approximately 960,000 Internet users in Ethiopia. Internet World Stats, "Ethiopia," 2012, http://www.internetworldstats.com/africa.htm#et (accessed July 8, 2013).

are located in Addis Ababa. According to the ITU, Ethiopia has some of the most expensive broadband in the world.[38] Given these costs, Ethiopians usually access the Internet through the growing number of cybercafés or from their mobile phones.[39] Internet has been available to mobile phone subscribers since 2009.[40] Wi-Fi Internet is increasingly available in many of the more expensive hotels and cafes. Connectivity speeds countrywide are quite low, and are prone to frequent outages.

The Ethiopian government has ambitious growth targets in the telecommunications sector. Ethiopia aims to increase mobile subscribers and mobile coverage six-fold over 2009-2010 levels by 2013-2014 and to increase Internet levels twenty-fold, according to Ethiopia's Growth and Transformation Plan.[41] The plan contains three key strategies for implementing this growth: telecom provider upgrades to meet international standards, the use of domestic products and services, and the "establishment and effective enforcement of comprehensive policy and regulatory frameworks to prevent and control illegal activities in the industry."[42]

Facebook use is growing more rapidly in many developing countries in comparison to more developed countries, where Facebook has a longer history of use. In Ethiopia, Facebook use is becoming increasingly popular with many of the young and educated to connect and share ideas and perspectives.[43] Despite legislative restrictions, Skype continues to be used widely.[44] Gmail, Hotmail, and Yahoo! Mail are the most popular

---

[38] Freedom House, "Freedom on the Net: 2011 Report," 2011, http://www.freedomhouse.org/report/freedom-net/freedom-net-2011 (accessed February 12, 2014) and ITU, "Measuring the Information Society," 2012, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf (accessed February 12, 2014).

[39] According to the ITU, Ethiopian mobile broadband subscriptions have increased from 0.1% in 2010 to 0.3% in 2011.

[40] Global Information Society Watch, "Ethiopia, 2009–Access to Online Information and Knowledge," 2009, http://www.giswatch.org/country-report/20/ethiopia (accessed August 3, 2013). For a discussion of internet costs throughout Africa, see ITU, "Measuring the information Society," 2012, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf (accessed March 14, 2014).

[41] Mobile subscribers, according to the Plan, are expected to increase from 6.5 million to 40 million, mobile coverage from 9 percent to 45 percent and Internet users from 187,000 to 3,690,000. The Growth and Transformation Plan is Ethiopia's economic development blueprint and covers 2010-2015. It contains ambitious growth targets in all key sectors. Ethiopia aims to be a middle income country by 2025.

[42] Federal Democratic Republic of Ethiopia, "Growth and Transformation Plan," 2010.

[43] While growing in popularity, only 1 percent of Ethiopians are on Facebook (902, 440 people according to Internet World Stats. Internet World Stats, "Ethiopia, Kenya," 2012, http://www.internetworldstats.com/africa.htm#et (accessed February 12, 2014). This compares to nearly 5% in Kenya. Facebook users are mostly urban, young and educated.

[44] Ethiopian law criminalizes the commercial use of Voice over Internet Protocol (VoIP) services (Internet-based voice services), while the government has stated that private use of Skype is still permitted. For a full discussion, see the section below, Internet Filtering.

webmail services and Paltalk is widely used in Ethiopia for group discussions.[45] Twitter has not been widely adopted.

Radio is still one of the most important mediums through which Ethiopians receive information. While television plays a larger role in urban areas, radio is still key in rural areas. One study found that 80 percent of Ethiopians use radio as a source of information while 53 percent said radio was their most important source of information. This study also reiterated the importance of word-of-mouth communication in Ethiopia, with nearly 50 percent identifying word of mouth as a source of information.[46] The radio and television sectors are dominated by government-affiliated stations. There are several private FM stations mainly focused on Addis Ababa affairs and no privately run television stations based within Ethiopia.

State Monopoly on Telecommunication Services

State-owned Ethio Telecom is the only telecommunications service provider in Ethiopia. It controls access to the phone network and to the Internet and all phone and Internet traffic must use Ethio Telecom infrastructure. There is no other service provider available in Ethiopia. Ethio Telecom therefore controls access to the Internet backbone that connects Ethiopia to the international Internet. In addition, Internet cafés must apply for a license and purchase service from Ethio Telecom to operate.

Ethiopia has been under pressure to liberalize its telecom sector from the World Bank and others to allow increased competition, but has thus far steadfastly refused to liberalize the sector.[47] Ethiopian Prime Minister Hailemariam Desalegn in mid-2013 resisted calls for privatization, calling the telecom sector "a cash cow for government coffers" and stressed that Ethio Telecom revenues were being used to fund the proposed Djibouti-Addis

---

[45] Paltalk is a video group chat service that allows large numbers of users to communicate via video, Internet voice, and chat. "Paltalk: Features," Paltalk, undated, http://www.paltalk.com/products.shtml (accessed February 11, 2014).

[46] Electoral Reform International Services, "Ethiopia Audience Survey 2011," 2011, http://www.eris.org.uk/images/userfiles/File/Audience%20survey%20report%202011%20Final.pdf (accessed October 4, 2013).

[47] Janelle Plummer, *Diagnosing Corruption in Ethiopia: Perceptions, Realities, and the Way Forward* (Washington, DC: World Bank, 2012), chapter 8, http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-9531-8 (accessed March 14, 2014).

railroad.[48] Ethiopia's desire to be a full member of the World Trade Organization (WTO) has renewed the calls for telecom liberalization.[49] However, Chinese telecom equipment giants ZTE and Huawei have been building and upgrading much of the country's telecom infrastructure since at least 2003.[50]

The desire to control the telecom sector has led to a grossly underdeveloped telecommunications system in comparison to regional neighbors.[51] This has the effect of stunting economic growth, particularly in rural areas, and limiting opportunities for the spread of ideas and information across the country.[52] But retention of this key sector allows government to more easily control and monitor who and how Ethiopians access the telecom and Internet services. The existence of private sector companies in the telecom sector could increase the difficulty for government of accessing communications records without going through additional steps or legal processes.

History of Telecommunications in Ethiopia

The Ethiopia Telecommunications Corporation (ETC) was originally established in 1952, and since that time has been Ethiopia's sole telecommunications provider. In 2006, ETC took a major step towards modernizing its outdated infrastructure, signing contracts worth US$2.4 billion with three major Chinese companies—ZTE, Huawei, and China International

---

[48] Andualem Sisay, "Ethiopia Telecom Sector to remain a monopoly," *Africa Review,* June 27, 2013, http://www.africareview.com/Business---Finance/Ethiopia-telecom-sector-to-remain-a-state-monopoly/-/979184/1896796/-/9hitv4/-/index.html (accessed July 2, 2013).

[49] "Ethiopia expected to join WTO in 2015: ministry," *Reuters*, July 2, 2013, http://www.reuters.com/article/2013/07/10/us-ethiopia-trade-idUSBRE9690BJ20130710 (accessed August 13, 2013).

[50] ZTE first entered Ethiopia in 1996. See Zhao Lili, "Contributing to the Development of Ethiopia with Wisdom and Strength," ZTE Tech, June 12, 2009, http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2009year/no6/articles/200906/t20090612_172517.html (accessed February 12, 2014).

[51] See Lishan Adam, "Ethiopia ICT Sector Performance Review 2009/2010," Research ICT Africa, 2010, http://www.researchictafrica.net/publications/Policy_Paper_Series_Towards_Evidence-based_ICT_Policy_and_Regulation_-_Volume_2/Vol%202%20Paper%209%20-%20Ethiopia%20ICT%20Sector%20Performance%20Review%202010.pdf (accessed February 12, 2014).

[52] Experiences in a range of countries show a strong connection between telecom privatization and rapid expansion of telecom infrastructure while various studies show a positive relationship between the expansion of telecom infrastructure and economic growth. See Carsten Fink, Aaditya Mattoo, and Randeep Rathindran (Development Research Group, World Bank), "An assessment of telecommunications reform in developing countries," *Information Economics and Policy*, no. 15 (2003), pp. 443-466. See also Lars-Henrick Roller and Leonard Waverman, "Telecommunications Infrastructure and Economic Development: A Simultaneous Approach," *The American Economic Review*, vol. 91, no. 4 (2001), pp. 909-923 and Anusa Datta and Sumit Agarwal, "Telecommunications and economic growth: a panel data approach," *Applied Economics*, vol. 36 (2004), pp. 1649-1654.

Telecom Corporation (CITCC)—to rapidly develop the country's telecommunications infrastructure.[53] As a result, these companies have played a large role in laying Ethiopia's main fiber optic communications network.[54] Prior to this time, Ethiopia's telecom infrastructure had been developed in an ad hoc manner by a number of foreign companies.

In addition, in 2006, ZTE signed a three-year, $1.6 billion deal to become ETC's sole equipment vendor for nine equipment packages.[55] The exact category of equipment sold under the deal is unclear, but ZTE was tasked with a major upgrade and expansion of both fixed line and mobile infrastructure and services. ZTE sells a range of telecommunications equipment, software, and services, including network switches, mobile handsets, and software systems.[56] As Zhang Yanmeng, chief executive officer of ZTE's Ethiopia subsidiary stated in 2009, "This is the world's only project in which a national telecom network is built by a sole equipment supplier."[57] Some have expressed concerns about the lack of transparency and heightened risk for corruption because of the nature of these deals.[58]

In December 2010, ETC became rebranded as Ethio Telecom, and outsourced management functions to France Telecom (now operating as Orange) via its subsidiary Sofrecom.[59] According to France Telecom-Orange (Orange), the objective of the management contract was to transform and modernize the operations of Ethio Telecom to "world class standards," including through capacity building for managers and transfer of know-how

---

53 Andualem Sisay, "Ethiopia Telecom Sector to remain a monopoly," *Africa Review*, June 27, 2013, http://www.africareview.com/Business---Finance/Ethiopia-telecom-sector-to-remain-a-state-monopoly/-/979184/1896796/-/9hitv4/-/index.html (accessed July 2, 2013) and Freedom House, "Freedom on the Net: 2011 report," 2011, http://www.freedomhouse.org/report/freedom-net/freedom-net-2011 (accessed March 14, 2014).

54 "ETC contracts Chinese trio for fixed and mobile expansion," *TeleGeography*, September 11, 2006, http://www.telegeography.com/products/commsupdate/articles/2006/09/11/etc-contracts-chinese-trio-for-fixed-and-mobile-expansion/ (accessed March 14, 2014).

55 See Plummer, *Diagnosing Corruption in Ethiopia*. See also, Zhao Lili, "Contributing to the Development of Ethiopia with Wisdom and Strength."

56 See ZTE Corp Snapshot, *Bloomberg Businessweek*, undated, http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?ticker=763:HK (accessed February 12, 2014).

57 Zhao Lili, "Contributing to the Development of Ethiopia with Wisdom and Strength."

58 Plummer, *Diagnosing Corruption in Ethiopia*; Lynn Hartley and Michael Murphree, "Influences on the Partial Liberalization of Internet Service Provision in Ethiopia," 2006, http://lilt.ilstu.edu/critique/fall2002docs/fall2006docs/Influences%20on%20the%20Partial%20Liberalization%20of%20Internet%20Service.pdf (accessed March 19, 2014).

59 Regulation 197/2010 Establishment of Ethio Telecom, governed by Public Enterprises Proclamation 25, 1992. Shareholders voted to formally rebrand France Telecom as Orange in 2013. Daniel Thomas, "France Telecom changes name to Orange," *Financial Times*, May 29, 2013, http://www.ft.com/cms/s/0/8f0926fe-c7b9-11e2-9c52-00144feab7de.html#axzz2w99PvfeT (accessed March 17, 2014).

and best practice.[60] Ultimately, the goal was to improve delivery of telecom services in Ethiopia and achieve "management autonomy" by the end of the contract.

Orange, through its subsidiary Sofrecom, was to oversee this broad restructuring of Ethio Telecom as part of the nationwide Business Process Reengineering (BPR) initiative, seen by many as the first steps towards privatization of Ethiopia's telecom operator.[61] The latest round of BPR in Ethiopia began after the 2005 elections and involved an overhaul of the structures and work processes of law enforcement, security, and other key institutions in an effort to improve efficiency.

By mid-2008, many of the BPR processes were completed nationwide, with staff reductions in many institutions. Former Ethio Telecom employees told Human Rights Watch of qualified personnel being removed from key positions because they were not EPRDF party members or because they questioned government policy.[62] They alleged that senior staff were often replaced by EPRDF cadres who did not seem to have the necessary qualifications.

In January 2013, Ethio Telecom's management agreement with Orange ended and Ethiopian managers, mostly EPRDF cadres, took over the key positions. Under Orange's management, telecommunications coverage in Ethiopia grew from 8 to 25 percent.[63] In the same period, the number of Ethio Telecom employees dropped from 12,600 to 8,600.[64] At the conclusion of the initial contract in December 2012, Orange and Ethio Telecom signed an additional one-year agreement, under which Orange would continue to provide support for "network design, architecture, technology selection negotiation and related technical areas."[65]

In June 2011, Ethio Telecom issued a tender inviting international suppliers to submit proposals to upgrade Ethio Telecom's infrastructure. Companies that registered interest

---

[60] Letter from Brigitte Dumont, Chief Officer, Group Corporate Responsibility, Orange, to Human Rights Watch, November 19, 2013.

[61] Business Process Re-Engineering (BPR) is the process of reorganizing how a company or public institution works, reviewing procedures, and reevaluating staff. For more information on Ethiopia's BPR program see Human Rights Watch, *Development without Freedom*.

[62] Human Rights Watch interviews, Kenya, Uganda, and United States, 2013.

[63] Meron Tekleberhan, "France Telecom Hands Over Administration of Ethio Telecom," *2Merkato*, January 4, 2013, http://www.2merkato.com/news/alerts/1956-france-telecom-hands-over-administration-of-ethio-telecom (accessed February 12, 2014).

[64] Ibid.

[65] Ethio Telecom, "The Management Contract with France Telecom Concluded," January 2, 2013, http://www.ethiotelecom.et/news/news.php?id=79 (accessed February 12, 2014).

included Ericsson, Nokia, ZTE, Huawei, and China International Telecom Corporation.[66] In August 2013 it was announced that ZTE and Huawei were the successful bidders in a $1.6 billion deal, though the exact details and breakdown of duties has not been announced.[67] Ethiopia's telecom infrastructure is outdated, but Ethiopia has ambitious plans to update that infrastructure through their partnership with ZTE and Huawei.

Institutions of Ethiopia's Telecommunication and Surveillance Apparatus

Until 2010, the **Ethiopian Telecommunication Agency (ETA)** was the government regulator for phone and Internet networks in Ethiopia that "specifies technical standards and procedures for provision of Telecommunications Services." It granted the ETC (now Ethio Telecom) a license in 2002 as Ethiopia's sole provider of telecommunication services and Internet services.[68]

The **Ethiopian Information and Communication Technology Development Agency (EICTDA)** played a key role in overseeing programs and polices related to information and communications technology (ICT) activities. EICTDA was formed in 2005 as an autonomous organization under the Ministry of Capacity Building. It formulated the National ICT policy in 2009, and managed the Woredanet program.[69]

The Woredanet program, which was partially funded by the World Bank and other donors, is intended to provide "ICT services such as video conferencing, directory, messaging and Voice Over IP, and Internet connectivity" to regional governments and local administrations throughout Ethiopia. According to government media, the program had reached 950 *woredas* and government offices by April 2013.[70] Cisco Systems, a US

---

[66] "Ethio Telecom Seeking New vendor Financers for Expansion," *Addis Fortune,* June 26, 2011, http://addisfortune.com/Vol_10_No_582_Archive/Ethio%20Telecom%20Seeking%20New%20Vendor%20Financiers%20for%20Expansion.htm (accessed February 12, 2014).

[67] "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 (accessed February 12, 2014).

[68] See Ethiopian Telecommunications Agency-List of Licenses at: Ethiopian Telecommunications Agency, "Licenses," undated, http://www.eta.gov.et/Licenses.html (accessed February 12, 2014).

[69] UN Public Administration Network, "WoredNet-Ethiopian Government Network," undated, http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan034887.pdf (accessed March 14, 2014).

[70] "Over 950 Woredas, Offices Benefit from Woredanet Project, Says Ministry of Information and Technology," *Waltainfo*, April 19, 2013, http://www.waltainfo.com/index.php/explore/8083-over-950-woredas-offices-benefit-from-woredanet-project- (accessed February 12, 2014); World Bank, "World Bank Provides US$50 Million for Public Service Delivery Improvement, Citizen Empowerment, and Good Governance Promotion in Ethiopia," March 23, 2010,

telecommunications equipment company, won a tender in 2003 to build the core network supporting WoredaNet and a related project, SchoolNet, which connects hundreds of secondary educational institutions across the country and provides access to the Internet and ICT equipment.[71] Subsequent projects also networked Ethiopian universities and equipped them with eLearning centers (UniversityNet) and connected agricultural centers (AgriNet) and hospitals (HealthNet).

The **Ministry of Communications and Information Technology (MCIT)**, formerly the Ministry of Information, assumed the responsibilities of both the ETA and EICTDA in 2010.[72] The MCIT is responsible for overseeing the implementation of communications and technology policies and programs in Ethiopia.[73] According to various former intelligence and Ethio Telecom officials, MCIT plays a major role in determining which radio and television programs are jammed and likely play a key role in determining which websites are blocked.[74] They are also responsible for the licensing of private media. The current minister is Debretsion Gebremichael, who replaced Bereket Simon, a longtime EPRDF member and advisor to the late Prime Minister Meles Zenawi. Debretsion is also one of the deputy prime ministers, the current chairperson of Ethio Telecom, and a former deputy director of NISS, underscoring the strong links between Ethio Telecom, the intelligence apparatus, and the Ministry of Communication and Information Technology. He was also the director-general of EICTDA during implementation of the Woredanet program and is a key TPLF member.

---

http://go.worldbank.org/VLCH71LCP0 (accessed March 19, 2014); Harry Hare, "Survey of ICT in Education in Ethiopia," *Survey of ICT and Education in Africa*, (Washington, DC: infoDev/World Bank, 2007), http://www.infodev.org/en/Publication.354.html;https://openknowledge.worldbank.org/bitstream/handle/10986/10671/463910BRI0Box31ia010ICTedoSurvey111.txt?sequence=2 (accessed November 8, 2013), p. Ethiopia-6; Lynn Hartley and Michael Murphree, "Influences on the Partial Liberalization of Internet Service Provision in Ethiopia," 2006, http://lilt.ilstu.edu/critique/fall2002docs/fall2006docs/Influences%20on%20the%20Partial%20Liberalization%20of%20Internet%20Service.pdf (accessed March 19, 2014).

[71] See Jason Deign, "Ethiopia Telecom's Next Generation Network Supports a Nation's Economic Transformation," News@Cisco, January 18, 2005, http://newsroom.cisco.com/dlls/2005/hd_011805.html (accessed February 12, 2014); Cisco, "Ethiopia Accelerates National Development Through Information and Communications Technology," undated, http://www.cisco.com/web/about/ac79/docs/wp/Ethiopia_SS_0320a.pdf (accessed February 12, 2014).

[72] Proclamation to Provide for the Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, No. 691/2010.

[73] Ministry of Communications and Information Technology, "About MCIT," undated, http://www.mcit.gov.et/?q=node/3 (accessed April 8, 2013).

[74] Human Rights Watch interviews, #11, 49, and 51, (locations withheld), July and August 2013.

The **National Intelligence and Security Services (NISS)** is Ethiopia's intelligence and security agency and has a broad mandate. While federal police and other law enforcement agencies have various roles and responsibilities in Ethiopia's security sector, the NISS takes the lead for any matters of national security and intelligence. It has always had a murky mandate. The July 2013 passage of the NISS Proclamation should have clarified that mandate, but the law contains vague language that gives NISS broad powers to investigate threats "against the national economic growth and development activities" and to gather intelligence on serious crimes and terrorist activities.[75]

The **Information Network Security Agency (INSA)**, a relatively new yet increasingly powerful branch of the security apparatus, was established to "ensure the security of information and information infrastructure to facilitate their use for the implementation of the country's peace, democratization, good governance, and development programs."[76] Accountable to the prime minister, INSA plays an important role in Internet monitoring and filtering of websites and is increasingly integrated with Ethio Telecom and other departments with information management mandates. It plays a key role in facilitating access to citizen's private digital communications for security and police forces, working closely with Ethio Telecom. INSA's role is constantly evolving and it is taking more and more responsibilities as Ethiopia's telecommunication sector grows.

In addition to various local informants, three main government departments are formally involved in intelligence gathering in Ethiopia: NISS, the Ethiopian Defense Forces (EDF), and the federal police. While the federal police have wide-ranging law enforcement responsibilities, federal police surveillance capacities are quite limited according to former federal police officials.[77] Together with NISS, the federal police form the joint anti-terrorism task force, although the federal police play a minimal role according to former officials.[78] This task force has been credited for foiling various alleged "terror plots," many of which led to the detention and subsequent charging of military officers, opposition politicians, and journalists both within Ethiopia and beyond. While federal police, regional police, or EDF soldiers have been present in many of the interrogations where phone

[75] National Intelligence and Security Service Re-Establishment Proclamation No.804/2013.

[76] Pursuant to Regulation 250-1011, Information Network Security Agency Re-establishment Council of Ministers Regulation.

[77] Federal Police Commission Proclamation # 313/2003.

[78] Human Rights Watch interview with former federal police official #11,(location withheld), February 2013.

records were inappropriately used, the vast majority of cases involved plainclothes security officials from NISS. Typically it is the NISS who most frequently uses copies of phone records and recorded phone calls during interrogations.

Although beyond the scope of this report, various former military officials told Human Rights Watch of the surveillance techniques and technologies used by the EDF. Most EDF intelligence gathering activities appears to be on external military targets whereas NISS focuses more on perceived domestic threats. There appears to be limited cooperation between the EDF and NISS over intelligence operations.

History and Background on Communications Surveillance

Phone wiretapping in its most traditional form involved physically attaching wires to the phone network to listen to private conversations.[79] This tactic has been in common and widespread use by law enforcement around the world for almost as long as phones themselves have been in use. Other devices can be used to capture information about the phone number associated with outgoing or incoming phone calls and time and duration of each call.[80]

Phone calls are connected through exchanges and switches located throughout a telecom network, which was once operated manually until more sophisticated switches were developed. While surveillance and data collection technologies were simple to implement by manually tapping wires or listening at centralized switches, collection and analysis remained time consuming and resource intensive.

Beginning in the 1990s, the widespread transition to digitally switched phone networks and growth of Internet networks made surveillance more complex to implement. However, new laws in the US and Europe boosted the use of wiretapping because it drove standardization of equipment for surveillance and enabled remote tapping of phone

[79] See Tom Harris, "How Wiretapping Works," *HowStuffWorks.com*, May 8, 2001, http://people.howstuffworks.com/wiretapping.htm (accessed February 12, 2014).

[80] Electronic Frontier Foundation, "Pen Registers" and "Trap and Trace Devices," Surveillance Self Defense, undated, https://ssd.eff.org/wire/govt/pen-registers (accessed February 12, 2014).

lines.[81] In the mid-1990s, the US and European governments began requiring telecommunications operators to make it easier for law enforcement to wiretap digital telephone networks.[82] In part, this took the form of legislation that forced companies to design modern networks and equipment to build in "back doors" that allow "lawful intercept" of communications on a larger scale.[83] This equipment became globally standardized and most telecom equipment sold around the world incorporates a range of surveillance capabilities as a result.[84]

Modern digital technology makes surveillance more powerful and efficient. The move from fixed-line to mobile telephone systems has enabled governments to access and collect a richer store of information about individuals. Mobile operators can enable interception of voice calls and facilitate access to SMS text messages they may retain.[85] Operators also routinely collect and store information that can reveal the location of a mobile phone, though the precision may vary. For billing and other purposes, telecom companies (fixed and mobile) create and maintain "call detail records," which list phone numbers of incoming and outgoing calls, call time and date, duration of calls, and mobile tower (location) information.[86] Moreover, mobile operators can be compelled to activate Global Positioning System (GPS) chips placed in most "smart phones," thus revealing the user's location and enabling prospective location tracking. Because mobile phones and SIM[87]

---

[81] See Whitfield Diffie and Susan Landau, "Internet Eavesdropping: A Brave New World of Wiretapping," *Scientific American*, August 22, 2008, http://www.scientificamerican.com/article.cfm?id=internet-eavesdropping (accessed February 12, 2014).

[82] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal C 329, at 0001 (Nov. 4, 1996), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML (accessed February 12, 2014); Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (Oct. 25, 1994), *codified at* 47 U.S.C. §§1001-10, http://askcalea.fbi.gov/calea (accessed February 12, 2014).

[83] "Lawful intercept" is an industry term that refers broadly to processes and technologies that enable law enforcement access to communications content on telecom networks. However, the exact contours of what is required (and under what legal process) will be defined differently in each jurisdiction. Use of the term does not necessarily imply that the surveillance itself is lawful under national law or international human rights law.

[84] Lawful intercept requirements in the US and Europe drove the global market for intercept-capable network equipment, while other countries began adopting similar lawful intercept laws.

[85] For background on mobile surveillance and network architecture, see Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair (accessed March 14, 2014).

[86] See for example, Aubra Anthony, "Call Detail Records: 'Does the NSA Know Where You Are?'" post to "Policy Beta" (blog), Center for Democracy & Technology, July 10, 2013, https://www.cdt.org/blogs/1007call-detail-records-%E2%80%9Cdoes-nsa-know-where-you-are%E2%80%9D (accessed March 14, 2014).

[87] A Subscriber Identity Module (SIM) card is a portable chip used mostly in cell phones that operate on the Global System for Mobile Communications (GSM) networks. The SIM card identifies and authenticates devices and subscribers on a cellular network.

cards each have unique identifiers, such data, when collected in bulk, can be used to create detailed dossiers of communications, associations, and movements over time, tied to specific individuals.[88]

Government surveillance and data collection has also shifted to Internet networks.[89] As the Internet enabled new channels for communicating and accessing information, it has also expanded the range and amount of information that can be monitored. New communications tools like Voice over Internet Protocol (VoIP) (voice calls made over Internet networks), chat, email, and social media services can be intercepted, though use of encryption can help shield online activity.[90] In addition, all Internet activity results in large amounts of "transactional" or "metadata," defined broadly as data *about* online activity.[91] For example, such data could include email addresses contacted, webpages visited, or Internet protocol addresses, or the geographic location of the parties communicating. Governments can collect this information easily by tapping networks or by compelling or asking companies to hand over data. When collected on a large scale, metadata can be highly revealing of a person's associations, movements, and activities over time.

As Internet access increases, some governments are adopting or compelling use of technologies like "deep packet inspection" (DPI). Deep packet inspection enables the examination of the content of communications (an email or a website) as it is transmitted over an Internet network. Once examined, the communications can be then copied,

---

[88] See Jessica Leber, "Mobile Call Logs Can Reveal a Lot to the NSA," *MIT Technology Review*, June 18, 2013, http://www.technologyreview.com/news/516181/mobile-call-logs-can-reveal-a-lot-to-the-nsa/ (accessed March 14, 2914; Ethan Zuckerman, "Me and my metadata – thoughts on online surveillance," post to "...My Heart's in Accra" (blog), July 3, 2013, http://www.ethanzuckerman.com/blog/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance/ (accessed March 14, 2914).

[89] See UN Human Rights Council (HRC), Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (Hereinafter, "Report of the special rapporteur on surveillance"), U.N. Doc A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed February 10, 2014).

[90] For example, using "https://" encryption when browsing websites that support the feature can help prevent eavesdroppers on the network from seeing the online content the user is viewing.

[91] See, "A Guardian Guide to Your Metadata," *The Guardian*, June 12, 2013, http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance (accessed February 12, 2014).

analyzed, blocked, or even altered.[92] DPI equipment allows Internet service providers—and by extension, governments—to monitor and analyze Internet communications of potentially millions of users in real time.[93] While DPI does have some commercial applications, DPI is also a powerful tool for Internet filtering and blocking and can enable highly intrusive surveillance.[94]

Finally, some governments have begun using intrusion software to infiltrate an individual's computer or mobile phone. Also known as spyware or malware, such software can allow a government to capture passwords (and other text typed into the device), copy or delete files, and even turn on the microphone or camera of the device to eavesdrop. Such software is often unwittingly downloaded when an individual opens a malicious link or file disguised as a legitimate item of interest to the target.[95]

In the near future, an increasing amount of data about individuals' communications, associations, location, and activities will be digitized. At the same time, the cost of computing and digital storage will continue to fall, enhancing governments' ability to collect and analyze electronic information. As access to mobile and Internet services increases, governments will be able to more efficiently and effectively intrude into the most sensitive aspects of peoples' private lives.

Phone calls, emails, and associations can be a valuable source of evidence to prosecute serious crimes and prevent legitimate threats to national security. However, surveillance and data collection, especially in bulk, is highly invasive of the right to privacy. International law requires surveillance practices to be regulated by law and subject to strong, independent safeguards to ensure they do not arbitrarily interfere with privacy.[96]

---

[92] In an analogy to physical mail delivery, an ISP (or government) using DPI would be the equivalent of the postal service opening an envelope to examine the contents of the letter inside, rather than limiting the ISP's role to examining the addresses on the outside of the envelope in order to deliver it to its destination.

[93] For background on DPI, see Alissa Cooper, "Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection," in *Privacy in America: Interdisciplinary Perspectives*, ed. W. Aspray and P. Doty (Plymouth, UK: Scarecrow Press, 2011), http://www.alissacooper.com/wp-content/uploads/2011/10/DPIchapter.pdf (accessed February 12, 2014).

[94] ISPs often use DPI to manage congestion on their network or to block spam and malware. However, there are less intrusive ways to achieve these aims. Ibid.

[95] See Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, April 30, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/ (accessed March 14, 2014).

[96] Report of the special rapporteur on surveillance.

II. Ethiopia's Control over Information and Communications Technology

The Ethiopian government exerts very tight control over all information and communications technologies through the deliberate jamming of radio and television signals, the monitoring of telephone calls and email communication, and by restricting access to information through blocking various Internet websites. The spread of telephone and Internet use in the country could open up opportunities to share ideas and information across geographical distances and borders in a manner that was inconceivable in Ethiopia a decade ago. But the government's use and control of this sector violates internationally protected rights to privacy and the freedoms of expression, association, and access to information. Sadly, Ethiopia's growing Internet and telecom sector, with so much potential to connect Ethiopians and open up access to new information, ideas, and opportunities, is being used as yet another tool against an already oppressed population.

Ethiopia's Growing Telephone Network: More Opportunities for Government Control?

Given Ethio Telecom's monopoly over the telecom system and recent technical upgrades enabled by foreign firms, the government of Ethiopia has the technical capacity to access virtually every single phone call and SMS message in Ethiopia. This includes mobile phones, landlines, and VSAT communications, and includes all local phone calls made within the country and long distance calls to and from local phones. Live interception capabilities are increasing and Ethiopia uses its exclusive control of the phone system to limit access to the network during sensitive periods.

Despite having almost unlimited control over the telecom network and the information that is being communicated on it, the ability to use those technologies acquired is limited and distrust between different officials and departments curtails the number of individuals with access to these surveillance capabilities. One former Ethio Telecom employee responsible for querying the Ethio Telecom database for specific phone calls estimated

that he received no more than 30 requests per month for these phone calls.[97] As mobile penetration and the government's surveillance capacity increases, the extent of unlawful surveillance may also increase.

International and national law relevant to Ethiopia's telecom and Internet surveillance are discussed in detail in the Legal Context section of this report. International human rights conventions to which Ethiopia is party, particularly the International Covenant on Civil and Political Rights, guarantee fundamental rights that have been repeatedly violated by improperly regulated government surveillance programs.

Under the 1995 Ethiopian constitution, everyone is entitled to the internationally protected rights to freedom of expression, to information, and to privacy. However, various national laws, such as the Mass Media and Freedom of Information Proclamation of 2008, the Telecom Fraud Offence Proclamation of 2012, and the Anti-Terrorism Proclamation, severely infringe on these fundamental rights. Human Rights Watch's research found, however, that many human rights violations related to the Internet and telecommunications in Ethiopia are not a product of abusive laws, but rather the willingness and ability of the authorities to act without being hindered by any legal framework or possible legal action from the country's criminal justice system.

"Brute Force" Confiscation

Despite these capabilities, the vast majority of individuals that Human Rights Watch interviewed who had experienced problems with the authorities from their telephone use were not from advanced surveillance technologies, but from security officials confiscating their mobile phone upon their arrest. Security officials, without warrants, would typically go through their phone log, their SMS messages, and sometimes their contact list. In some cases, this was to verify information that security officials already seemed to know but in most cases officials seemed to be acquiring new information. While some of the individuals who were subject to this unsophisticated but effective technique were in remote, rural areas and not high-profile, some very high-profile individuals were subject to this basic technique. In some cases, security officials knew the phone numbers of the people they were interrogating, but in many cases they did not. Given that Ethio Telecom

[97] Human Rights Watch interview with former government employee #100, (location withheld), October 2013.

has a comprehensive database of names, phone numbers, and other personal information of all phone owners in Ethiopia, it is clear that many security officials do not have regular access to the information contained in this database.[98]

One high-profile case highlighted the relatively unsophisticated use of the telecom system. In February 2009, US diplomat Brian Adkins was found murdered in Ethiopia.[99] According to former federal police officials, the police retrieved his telephone and went through the last phone numbers he had called. Using the Ethio Telecom database, they cross-referenced the phone numbers to the names and home addresses of these individuals. They interrogated each of them and eventually one of them confessed and was sentenced to 17 years in prison.[100] There was no attempt to access the phone records of these individuals, no attempt to determine the locations of callers, and no attempt to listen to the phone calls between Adkins and these individuals. These capacities all exist within Ethio Telecom's systems. Despite the technologies existing and being available, only rudimentary techniques were used for this high-profile case.[101]

Unrestricted Access to Phone Call Recordings and Metadata

Perhaps the most blatant misuse of the telecom system is the government's ease of access to historical phone records and recorded calls of Ethio Telecom customers and other metadata.[102] Ethiopian security officials can access the records of all phone calls made inside Ethiopia with few restrictions. Information on all phone calls is stored and easily accessed through Ethio Telecom's customer management system, ZSmart. ZSmart is a customer management database developed by ZTE and installed for Ethio Telecom to manage all aspects of a customer's account, from personal information (name, address, even ethnicity) to billing information and detailed listings of phone calls.[103] Phone call

---

[98] Human Rights Watch interview with former government employee #49, (location withheld), May 2013.

[99] Hanna Ingber Win, "Brian Adkins, US Diplomat, Killed in Ethiopia," *Huffington Post*, March 8, 2009, http://www.huffingtonpost.com/2009/02/05/brian-adkins-us-diplomat_n_164270.html (accessed April 3, 2013).

[100] Desalegn Sisay, "Ethiopian Man, jailed over US diplomat's murder, claims 'rape,'" *Afrik News,* July 15, 2009, http://en.afrik.com/article15924.html (accessed March 14, 2014).

[101] Human Rights Watch interview with former government employee #11, (location withheld), February 2013.

[102] Phone metadata can be defined loosely as information about a phone call like call time, duration, and numbers dialed, but not the content of the voice call itself.

[103] Human Rights Watch interview with former government employee #49, May 2013. ZTE offers a range of ZSmart products, from customer billing, technical support, marketing, and fraud detection functions. See, for example, ZTE, "ZTE Launches ZSmart Intelligent Charging System (iCS)," May 22, 2012,

information includes the originating and receiving phone numbers, the location of originator/receiver, the time, date and duration of every call.[104] ZSmart also includes the content of SMS text messages and the audio of phone calls received or originating from a selected phone number can be recorded, which can then be easily downloaded and listened to or saved to a USB stick for future use.[105]

While standard, off-the-shelf customer management and billing systems have legitimate purposes, the ease of access by security agencies and lack of procedural or legal constraints, means that the system can be misused in inappropriate ways to access information that should remain private. That the ZSmart system in Ethiopia has been configured to enable access to text messages and full recordings of phone conversations only exacerbates the risk of abuse. ZSmart has been in place since 2009.

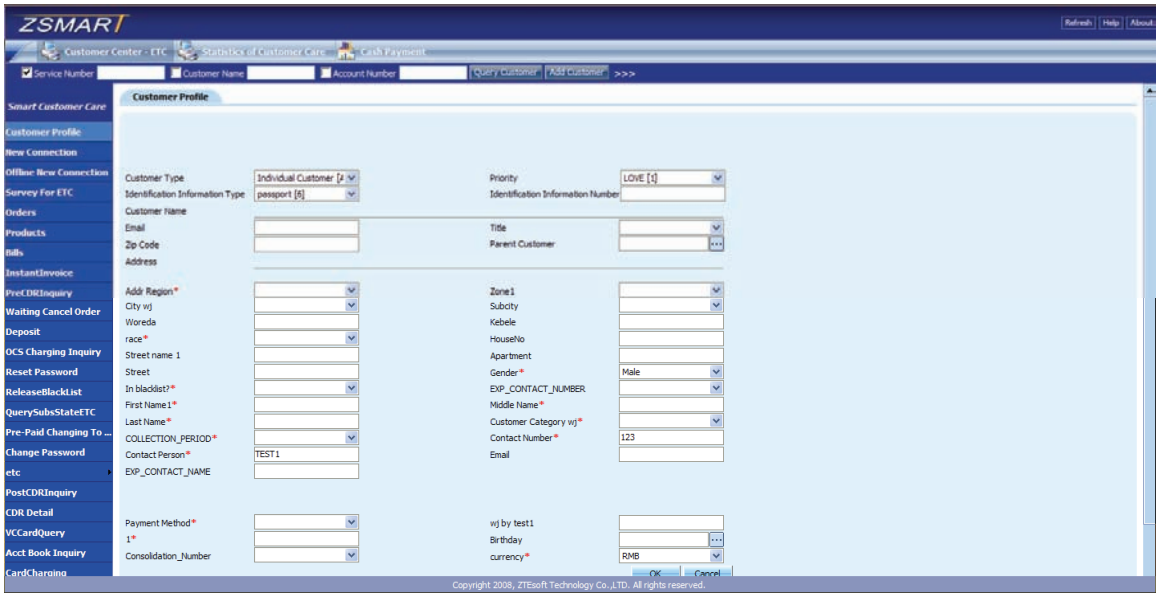


Figure 1. Sample screen from Ethio Telecom's ZSmart database. Required fields include name, gender, race, and whether the individual is on a "blacklist."

---

http://www.zteuk.co.uk/news/news/201205/t20120522_12830.html; ZTE, "OSS/BSS VAS Solutions," 2014, http://wwwen.zte.com.cn/en/solutions/anyservice/oss_bss/ (accessed October 24, 2013). "Ethnicity" is one of the required fields in ZSmart. This raises concerns about possible discrimination against certain ethnicities, an ongoing allegation against the government. The overwhelming majority of individuals Human Rights Watch found who have experienced abuses through their use of the telecommunications system were from one ethnicity.

[104] Human Rights Watch interview with former government employee #49,(location withheld), May 2013.

[105] Ibid.

All telecom companies globally maintain some level of record keeping of customer phone use for a variety of valid business reasons—otherwise, customer billing would be difficult to track.[106] Crucially, however, capturing a recording of phone calls or the content of text messages is not necessary for these business functions.

Government access to the content of phone calls, text messages, and metadata/call records interferes with the right to privacy. As a result, to ensure such interference is not arbitrary or unlawful, many governments have enacted laws that restrict access to phone records and the circumstances in which calls can be intercepted or recorded. In many countries, it is illegal to record a phone call without a judicial warrant. Security or law enforcement agencies are often required to go through a specified legal process and demonstrate a legitimate aim, under oversight by an independent authority. A legislative framework that regulates access to this information is needed to protect the right to privacy and ensure that access to this information is undertaken in a proportionate and legitimate manner on appropriate targets and only by specified, authorized individuals.

The framework for legal protections of privacy rights in Ethiopia is limited. While laws exist that provide some guidance for surveillance (requiring the issuance of warrants for certain kinds of searches, for example), Human Rights Watch has found no indication of any regulations, directives, or procedures that guide surveillance and intelligence gathering beyond this. Our investigations did not uncover a single case in which there was evidence that warrants were issued by the courts to facilitate access to phone records or recordings.

Former Ethio Telecom and security officials told Human Rights Watch that the lack of defined rules and procedures meant that anybody with appropriate ZSmart database permissions could easily access this information. Former Ethio Telecom employees said that no request for information from NISS had ever been denied as far as they were aware.[107] Federal legislation requires that Ethio Telecom cooperates with NISS when they are requested to provide intercepted information.[108]

---

[106] Operators generate a "call detail record" for each call made. These records include details necessary to determine, for example, the number of minutes used and whether it was a local or long-distance call, which then allows the operator to charge their customer appropriately.

[107] Human Rights Watch interview with former government employee #101, (location withheld), October 2013.

[108] The anti-terrorism proclamation requires Ethio Telecom to "cooperate when requested by the National Intelligence and Security Service to conduct the interception," (art. 14(3)) and imposes a general duty on government and private entities to

In practice, private customer information was accessed by security and intelligence officials in a variety of ways. Federal police officials would typically present letters to Ethio Telecom senior managers for access to certain user information. These letters were not signed by the courts and no rationale or legal justification for the request was ever given. These letters would then be passed on to junior Ethio Telecom officials by senior managers to facilitate the requests. NISS requests for phone records were much more informal: they would either communicate orally to Ethio Telecom employees whom they had established a relationship with to access certain information, or would show up at Ethio Telecom offices to query ZSmart themselves using log-in credentials supplied by Ethio Telecom employees. Ethio Telecom employees, fearful of reprisals from security officials, comply with these requests. NISS does not appear to go through a particular hierarchy or formal process to access customer data or phone call recordings.

Former Ethio Telecom employees also explained that the process for selecting targets of surveillance was often similarly informal. Authorities would provide specific telephone numbers to select for the recording of phone calls through the ZSmart system. Once a number is selected for surveillance, all calls made to and from that number would be recorded and accessible through ZSmart. Authorities rarely requested an end to recording of calls once a number was selected for surveillance.[109]

Numerous individuals said that security officials told them that they were being continuously monitored. Those officials would then show them information from their phone records during interrogations. Often security officials were using this information to find out the location of different individuals they were looking for who communicated by phone with the detainee. Other times they wanted to clarify the meaning of the contents of specific phone communications. Several individuals told Human Rights Watch in detail about specific information gleaned from recorded phone calls that security officials revealed during interrogations.

One member of the Oromo National Congress, a registered Oromia-based political party, who was tortured in detention, describes his 2010 arrest:

---

disclose information that could assist with investigations (art. 22). The recently passed NISS Proclamation has similar requirements with those refusing to cooperate punishable according to the Criminal Code (art. 27).

[109] Human Rights Watch interview with former government employee #49, May 2013.

> After some time I got arrested and detained. They had a list of people I had spoken with. They said to me, "You called person x and you spoke about y." They showed me the list—there were three pages of contacts—it had the time and date, phone number, my name, and the name of the person I was talking with. "All your activities are monitored with government. We even record your voice so you cannot deny. We even know you sent an email to an OLF [Oromo Liberation Front] member." I said nothing. "I have a right to be a party member, I have a right to contact ONC. This is not a crime." I refused to acknowledge I was OLF because I am not. They put me in cold water and applied electric wire onto my feet, they plugged the wire into the wall. They wanted me to admit that different people I had called were OLF and I told them I do not know if they are or not, which was true. They played one call with an Oromo where I said, "How are we going to meet?" "That means you are planning something" is what they told me. That was not a crime, they were a member of my party—I needed to speak with them.[110]

An Oromo artist who wrote about political issues was charged under the Criminal Code after being accused of being a member of the OLF along with several dozen other people.[111] She described her interrogation in Makalawi prison in Addis Ababa:

> I was presented a six-page list of phone calls. They had calls highlighted and asked me specific questions about those calls. They also had my email address and showed me it but I denied that I had an account. They put a gag in my mouth and tied my hands behind my back to the chair I was sitting on. They said, "You spoke with somebody called [Oromo name] at time x from place y." Many of these calls were to people in Moyale.[112] They told me to confess I was OLF. They pushed me on this every night for one month.… When I wouldn't confess they kept going back to my list of calls, and wanted to know who different people were. They played several phone calls I had with friends demanding to know what I meant when I said

[110] Human Rights Watch interview #61 (name and location withheld), July 2013.

[111] She was charged under sections 241 32(a), 32(b), and 38(1) of the Criminal Code.

[112] Moyale is a town on the Kenya/Ethiopia border and is often the gateway for Oromos who are fleeing Ethiopia into Kenya. The area around Moyale has a high Oromo population.

> different things. I had nothing to tell them, we were just arranging to meet up. They kept telling me, "All your activities are monitored."[113]

The phone call recordings were not used in court and the defendants were all convicted and sentenced under various provisions of the Criminal Code. On appeal, her sentence was substantially reduced because of lack of evidence.[114]

Another Oromo man described the authorities' use of phone records against him:

> Eventually I was detained. "You have been communicating with a, b, and c. You are collecting money for students and giving to OLF." It was a plainclothes security man who detained me in Moyale and took me to the local police station and asked me all these questions. I was scared. "If you are talking through this telephone we record all conversations." They mentioned around five peoples' names I had been communicating with. They described in detail what I was saying to these people. On those calls, I talked about the constitution, about international human rights law, and how it exists only on paper. Government is not doing any of this. They told me this was considering "mobilizing" and that was why I had been arrested.[115]

A journalist who was arrested after a demonstration in Oromia said he was mistreated in a military camp because he was communicating with "enemies of the government." His 2012 telephone records were used to monitor his activities. He described the experience to Human Rights Watch:

> A demonstration was being planned in (name withheld). I went and recorded video of the demonstration as I was instructed. We were targeted because of this. They smashed our camera. Our press manager was arrested at the demo, they followed me home and arrested me there and many of my other colleagues were arrested as well. I was taken to (name

[113] Human Rights Watch interview #89 (name withheld), Kenya, July 2013.
[114] Translated charge sheet and decision, on file with Human Rights Watch.
[115] Human Rights Watch interview #60 (name withheld), Kenya, July 2013.

> withheld) military camp. "All your records belong to us. You talked to x, a Muslim activist. You talked to person y, he is OLF." I think they mentioned five people inside the country, and six or seven outside. "Since you started your job, we monitor all your activity. We know everything." The ones outside [of Ethiopia] were all friends and family … the five inside [Ethiopia] were all from work.[116]

Several individuals told Human Rights Watch that recordings of their intercepted phone calls were played for them by security officials during their interrogations. These phone calls were played from a memory stick or direct from a laptop and were only played after the detainees refused to divulge what they were communicating to certain individuals. In each of these cases, detainees describe innocuous information being twisted, invariably to try to link individuals to banned organizations, usually either Ginbot 7 or OLF. Quite often individuals were accused of "mobilizing" individuals to join the OLF. Most of these detained individuals were involved in registered Oromo opposition parties—often ONC or OPC.[117]

Despite the extensive use of phone records during interrogations, the use of phone records or phone conversations in trials is much more limited. The 2011 anti-terrorism trials of Reeyot Alemyu, Eskinder Nega, and others featured recordings of phone calls introduced as evidence in court. In Eskinder's case, the phone calls were with Elias Kifle (editor of Ethiomedia, a website run from the United States), Ethiopian Satellite Television (ESAT) journalist Abebe Belaw, and opposition party leader Andualem Arage.[118] Elias, Abebe, and Andualem were all also convicted under the anti-terrorism law.[119] According to court records, other introduced electronic evidence included Facebook and email communications between the defendants and the leadership of Ginbot 7.[120] Phone calls introduced as

---

[116] Human Rights Watch interview #62 (name withheld), Kenya, July 2013.

[117] The Oromo National Congress (ONC) is a registered political party founded in 1996. After the 2005 elections, the National Electoral Board of Ethiopia awarded the names of the ONC and the Coalition for Unity and Democracy (CUD) to government-allied groups. See generally, Human Rights Watch, *"One Hundred Ways of Putting Pressure,"* p. 16. The ONC then changed its name to the Oromo People's Congress (OPC).

[118] Translation of charge sheet, on file with Human Rights Watch.

[119] Elisa Kifle is the editor of Ethiomedia, a diaspora based news site that is often critical of the EPRDF.

[120] Ethiopian Terrorism Trial Hears Journalist Defendant," *Voice of America*, March 27, 2012, http://www.voanews.com/content/ethiopian-terrorism-trial-hears-journalist-defendant-144654675/179445.html (accessed February 13, 2014). Various emails were also introduced as evidence but not clear how these emails were obtained. Several witnesses suggest Eskinder gave up his password but not clear under what circumstances he did this. Translation of charge sheet, on file with Human Rights Watch.

evidence in Reeyot's trial were also with Elias Kifle.[121] All phone calls introduced as evidence involved the phone calls of one of three people: Eskinder Nega, Andualem Arage, or Kenfemichael Debebe.[122] Under the anti-terrorism law, court warrants are required for access to this information. It is not clear whether any warrants were acquired.

The vast majority of the cases documented by Human Rights Watch involving access to phone recordings involved Oromo defendants organizing Oromos in cultural associations, student associations, and trade unions. No credible evidence was presented that would appear to justify their arrest and detention or the accessing of their private phone records. These interrogations took place not only in Addis Ababa, but in numerous police stations and detention centers throughout Oromia and elsewhere in Ethiopia. As described in other publications, the government has gone to great lengths to prevent Oromos and other ethnicities from organizing groups and associations.[123] While the increasing usefulness of the mobile phone to mobilize large groups of people quickly provides opportunities for young people, in particular, to form their own networks, Ethiopia's monopoly and control over this technology provides Ethiopia with another tool to suppress the formation of these organizations and restrict freedoms of association and peaceful assembly.

Human Rights Watch interviews revealed that interrogations seem to follow a similar pattern in which individuals are repeatedly told that security "is monitoring everything" and they should confess to various charges. If confessions are not forthcoming, security officials reveal knowledge of individual phone calls. If a confession or information is not revealed then an entire list of phone calls is produced or an individual phone call is played. At this stage, if no confession or information is obtained, prolonged detention takes place. As is often the case in Ethiopia, arbitrary detention without formal charges is common. In the cases Human Rights Watch has documented, mistreatment in detention at this stage frequently occurs.[124]

---

[121] Email correspondence was also introduced including communication with Elias and various communications surrounding the *Beka* movement.

[122] Translation of charge sheet.

[123] Human Rights Watch, *Suppressing Dissent*.

[124] Human Rights Watch, *They Want a Confession: Torture and Ill-Treatment in Ethiopia's Maekelawi Police station*; "Ethiopia: Political Detainees Tortured," Human Rights Watch news release, October 18, 2013, http://www.hrw.org/news/2013/10/18/ethiopia-political-detainees-tortured.

Human Rights Watch wrote to ZTE to verify ZSmart's capabilities and inquire about ZTE's role in installing or training employees on this system in Ethiopia, as well as the firm's policies to prevent abuse of its technologies. Human Rights Watch received no response to its letter and follow-up email, other than an acknowledgment of receipt. While ZTE's public reports state that it has a corporate social responsibility strategy, including a Code of Business Conduct, it is unclear whether ZTE has any human rights policies in place to respect the right to privacy and freedom of expression.[125]

Human Rights Watch also wrote to France Telecom-Orange about its role in implementing or updating the ZSmart system, and asked whether the company raised privacy issues related to access to metadata and recorded phone calls. Orange stated that its subsidiary Sofrecom was not involved in the selection of Ethio Telecom's ZSmart customer care and billing system, nor in the selection or implementation of security equipment for mobile or Internet networks in Ethiopia.[126] Orange specified that its only role was to ensure implementation for the customer care and billing system was done according to "industry best practices" to prevent unauthorized intrusion into the system. The firm has not been involved in discussions with the government concerning law enforcement access to user data. Finally, Orange confirmed that in a typical customer care and billing system, there is no need to record the content of phone calls.[127]

The ease of access to the phone records and intercepted calls of ordinary Ethiopian citizens without any safeguards is contrary to the rights to privacy enshrined in the Ethiopian constitution of 1995 and international law.[128] While legislation exists that enables access to phone records with a court warrant (or requires a warrant for generically defined "searches"), the law is vague or sometimes deficient in what it requires law enforcement and security agencies to prove to obtain a warrant.[129] In any case, these provisions by all accounts are ignored in practice and security officials access records with

[125] ZTE, "About ZTE: Responsibility," 2014, http://wwwen.zte.com.cn/en/about/corporate_citizenship (accessed March 20, 2014).
[126] Email from Yves Nissim, VP, Head of Transformation and Operation in CSR, Orange Group, to Human Rights Watch, February 14, 2014.
[127] Ibid.
[128] See below, Legal Context.
[129] See, e.g., Anti-Terrorism Proclamation, art. 14, 23; NISS Re-establishment Proclamation, arts. 8, 22-24; Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation arts. 25 and 52; Telecom Fraud Offence Proclamation, arts. 14-16.

little reasonable justification for their actions. Ethio Telecom officials said they could not resist government requests to hand over phone records because of fear of reprisals. As Ethiopia targets ambitious growth in its telecom sector, the problems arising from these issues are likely to multiply unless seriously addressed.

Targeting Foreign Communications

The Ethiopian government has also made use of the telecom system to arbitrarily arrest and detain individuals in Ethiopia shortly after those individuals communicated by phone with individuals outside the country. These arrests take various forms. In some of the 14 credible cases reported to Human Rights Watch, the authorities arrest people after they received phone calls from specific individuals (linked to specific phone numbers). In other cases they are arrested immediately after receiving phone calls from specific countries shortly after a friend or family member wanted by security had fled Ethiopia into that particular country. And in other cases, people that were already being harassed by security were arrested after they received a phone call from an unknown person from outside of Ethiopia. In the majority of these cases, security officials state communication with "OLF operatives in [country x]" as the basis for the arrest.

In some cases, individuals had their phones confiscated by security officials who went through the phone's call log to check details of who they communicated with and that individual was arrested once it was evident a call had been received from outside of Ethiopia. In many other cases, security officials showed up at the individual's home or place of residence between several hours and several days later and arrested them stating it was because of their out-of-country phone communication. While Ethiopia has information about the owner of every Ethiopian phone number (because of mandatory SIM card registration), it does not have the same information on foreign numbers. All Ethio Telecom can determine is the phone number, and thus the country of origin through the country code.

Many Ethiopians living outside of Ethiopia told Human Rights Watch of their fear of calling friends and relatives in Ethiopia because of this possibility. Many of them have been told by their family members not to call or communicate anymore because it is putting them at risk. While it is difficult to corroborate all of these cases, there are enough credible cases to indicate this is being used as a strategy to limit communication with individuals outside

of Ethiopia. This also shows how telephone metadata can be used by the government as proof of a "crime."

The majority of cases that Human Rights Watch investigated concerned communications with Oromo individuals in Kenya. However, there were several incidents of arrests as a result of calls to the Gulf States, to the United States, and to other sub-Saharan African countries. The vast majority of Oromos who flee Ethiopia go through Moyale in southern Ethiopia, and the borderlands between Kenya and Ethiopia are believed to be a base for OLF fighters. A presence among and perceived support for the OLF in Kenya's Oromo refugee community is no justification for arresting Ethiopians who communicate with Ethiopian refugees abroad. Individuals also told Human Rights Watch that they believed foreign phone numbers were being targeted for a variety of reasons including the Muslim protests, money laundering, corruption, and to reduce the likelihood of further migration out of Ethiopia.

One high-profile case involved a United Nations security officer Abdirahman Sheikh Hassan, who was convicted in June 2012 and sentenced to seven years and eight months under the anti-terrorism law. According to media reports, the key evidence against Hassan were transcripts of phone conversations between Hassan and Sherif Badio, an ONLF leader in Australia, while he was trying to negotiate the release of two UN World Food Program workers kidnapped by the ONLF in May 2011.[130]

Live Interception of Phone Communication

A number of individuals spoke to Human Rights Watch about the perception that phone calls are being monitored in real-time. While former intelligence officials confirmed that INSA has the technical capacity to do this, there is little evidence that it is done with regularity. Given the large volume of phone calls and the variety of different languages used in Ethiopia, it seems unlikely that live interception is occurring with any but the most critical of targets. Former Ethio Telecom officials told Human Rights Watch that Ethio Telecom employees do not have the capability to listen to the content of live mobile phone calls—that capability is restricted to INSA.

---

[130] "Ethiopian UN Security Official on Trial for Terrorism," *Voice of America,* April 8, 2012, http://www.voanews.com/content/ethiopian-un-security-official-on-trial-for-terrorism-146744295/181000.html (accessed May 2013); "UN Staff Union seeks release of workers detained in Ethiopia, Sudan," *Xinhua News Agency*, May 1, 2012, http://news.xinhuanet.com/english/world/2012-05/01/c_131561279.htm (accessed March 14, 2014).

One former Ethio Telecom official described the pressure he was under to listen and record VSAT communication from a town in southern Ethiopia. He refused and said he was arrested three times for refusing to record conversations. In one case, the US broadcaster Voice of America (VOA) and German broadcaster Deutsche Welle were communicating with people about local political issues through Ethio Telecom's VSAT satellite phone, the only phone in the community.[131] He had been told he had a responsibility to monitor who uses the phone and to record "relevant" phone calls. He did not do that and was arrested. When he was posted to another location, security officials would give him specific phone numbers to monitor and record. He refused. When farmers from that *kebele* started appearing on VOA and Deutsche Welle, he was removed from his job and arrested.[132]

Other individuals described to Human Rights Watch how their phone calls were diverted to third parties in often bizarre ways. Sometimes individuals would call a number and someone else would pick up the phone and query them on why they were trying to call this number. In other cases, the call would go through to the intended recipient, but a third individual interjects, insulting or asking follow-up questions. In these cases, the individual who answered knew details about the identity of the caller.

In all of the above cases, individuals had been under threat from security officials in the days leading up to these incidents and many had been arrested previously, usually without charge. While these anecdotal examples illustrate crude uses of this technology, they are indicative of the ability to divert and listen to phone calls, something that was corroborated by former intelligence officials.

Restricting Access to Phone Network

Since Ethio Telecom is the only service provider in Ethiopia, should a SIM card or phone number be blocked by Ethio Telecom, then that individual cannot access phone services in Ethiopia. The UN special rapporteur on freedom of expression has called on governments

[131] VSAT is a satellite-based telephone service that is used to connect small remote areas to the Ethio Telecom infrastructure without the need of physical connection to the infrastructure. Ethiopians can use phones connected by Ethio Telecom offices in remote areas. As mobile coverage increases across Ethiopia, VSAT is being phased out.

[132] Human Rights Watch interview #39 (name and location withheld), May 2013.

to refrain from compelling SIM card registration since it creates barriers to access to telecom services that are vital for a range of rights.[133]

In order to receive a SIM card, individuals must produce government-issued ID, a passport-sized photograph and submit personal information (including home address and ethnicity). SIM cards are granted either through Ethio Telecom or through Ethio Telecom authorized resellers. Given Ethio Telecom's monopoly over the sector, there is no other way to acquire a SIM card. Prevalence of mandatory SIM card registration has grown dramatically in Africa in recent years, with 48 African countries requiring mandatory registration of SIM cards.[134] However, mandatory, real-name registration of SIM cards is not standard procedure in many other countries around the world, including in the US.

While there could be a commercial or technical justification for a certain phone number being blocked, there is no evidence of a policy or procedure to guide when and why a phone number may be blocked by security officials.[135] It largely seems to be up the whim of security officials who communicate the requirement to be blocked to EPRDF cadres within Ethio Telecom, who either update ZSmart accordingly or orally share this information with frontline employees.[136]

Many individuals described to Human Rights Watch that after they were arrested or interrogated about their phone communications, their SIM cards no longer worked. Fearful, most of these individuals stopped using their phone altogether, others borrowed friends' phones to make calls, and others went to Ethio Telecom to find out why their SIM card no longer worked.

Some individuals who were blocked and tried to acquire another SIM card were told by Ethio Telecom that they were not permitted to get another SIM card. Because Ethio Telecom maintains a database of all SIM cards cross-referenced with names and personal

---

[133] Report of the special rapporteur on surveillance, para. 88.

[134] Carly Nyst, "With new promise comes new perils: ICTs and the right to privacy in Africa," Privacy International, November 30, 2012, https://www.privacyinternational.org/blog/with-new-promise-comes-new-perils-icts-and-the-right-to-privacy-in-africa#footnote3_3s6169 (accessed March 14, 2014).

[135] For example, a phone number or SIM card may be blocked if a phone has been reported lost or stolen to prevent unauthorized use of the phone or card.

[136] Human Rights Watch interview with former government employee #100, (location withheld), October 2013.

information, they can easily prevent a blocked individual from acquiring another SIM card.[137] This effectively restricts the blocked individuals' rights to freedom of expression and association.

While the extent of SIM card blocking cannot be ascertained, Human Rights Watch did not find evidence that it was widespread. In the cases Human Rights Watch documented, SIM card blocking may have been used by the government only after other methods of intimidation and threats did not have the desired outcome.

The prevalence of Ethiopia's *kebele*-level surveillance system ensures that people limit where and when they communicate with each other at a local level. Because of practical and administrative challenges with traveling to neighboring villages, opportunities to communicate between different geographical areas were limited prior to the growth of Ethiopia's telecom network. The newfound prevalence of the mobile phone, and VSAT prior to that, have allowed individuals to communicate across geographic distances, resulting in the spread of ideas, news, and increasing the possibility of intra-*kebele* collaboration on various issues. While there are many economic and technical barriers that limit the usefulness of this technology for rural Ethiopians, limiting access to the telecom system prevents individuals from sharing ideas and mobilizing across distances in the same way that grassroots systems of surveillance always have. Given Ethiopia's monopoly over the telecom sector, those individuals who do not have access to the telecom system or cannot get a SIM card have no other option to turn to as there are no other telecom providers in Ethiopia.

Network Shutdowns

There have also been numerous occasions in which Ethiopia has shut down the phone network or SMS capabilities in certain locations at certain times. Given Ethiopia's control over the telecom sector, the government can very easily turn off phone and Internet networks whenever it perceives a threat. It has used this ability to impact peaceful protests throughout the country, during counter-insurgency operations in the Ogaden, and during and after sensitive elections. One ONLF member described how they always knew an Ethiopian military offensive was imminent because the mobile network would be suddenly

[137] As seen in Figure 1, Information provided to Human Rights Watch clearly shows that Ethio Telecom's customer management system ZSmart has a field for identifying a whether a SIM card has been blocked: "Is blocked?"

unavailable in the area of the offensive. Once the offensive was complete, mobile service would resume.[138] In the violence that followed the 2005 federal elections, the government took the unprecedented step of blocking access to SMS and only resumed the service in September 2007, alleging that the opposition had been using SMS to organize protests.[139]

One former Ethio Telecom engineer described to Human Rights Watch the ease of turning off the network for specific times and in specific locations. As an example of the precision of this technique, when key foreign dignitaries drive from the airport in Addis on the main Bole Road to the presidential palace, the mobile towers along the route are turned off five minutes before the motorcade arrives and resume shortly after they pass each tower. Federal police and security officials combine their efforts along the route until the head of state has passed.[140]

A former government employee from East Harerghe Zone in Oromia described the disruption to telecom service that would occur at politically sensitive times:

> Whenever a demonstration is planned, the telecom service in eastern Harerghe is cut. During local elections it was cut. During recent Muslim protests it was cut. It is usually cut from 6 a.m. until after 2 p.m. Message I would get in Amharic is "for time being there is no service." Our network comes and goes all the time, but as soon as there is a problem for government there is no service whatsoever.[141]

In Ethiopia, available legislation does not address when the government may shut down networks, and under what legal process or safeguards. Instead, the availability of the

---

[138] Human Rights Watch interview #47 (name and location withheld), May 2013.

[139] Global Information Society Watch, "Ethiopia, 2009 – Access to Online Information and Knowledge," 2009, http://www.giswatch.org/country-report/20/ethiopia (accessed August 3, 2013). A small number of governments have shut down mobile or Internet services at such large scale—that is, on a regional or nationwide level—often in response to demonstrations or unrest. See OpenNet Initiative, "Global Internet filtering in 2012 at a glance," April 3, 2012, https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance (accessed February 12, 2014); David Sullivan, "Network Shutdowns Go Beyond Syria," post to Future Tense (blog), *Slate*, May 9, 2013, http://www.slate.com/blogs/future_tense/2013/05/09/internet_shutdowns_go_beyond_syria.html (accessed February 12, 2014).

[140] Human Rights Watch interview with government employee # 14, (location withheld), February 2013 and Human Rights Watch interview #2 (name withheld), Kenya, November 2012.

[141] Human Rights Watch interview #78 (name and location withheld), July 2013.

mobile network is subject to the whim of government officials who frequently impose unlawful restrictions on public gatherings.

The special rapporteur on freedom of expression has criticized the use of network shutdowns as a violation of the right to freedom of expression.[142] Given the increasing importance of mobile phones in Ethiopia, turning off the mobile network provides the Ethiopian government a further means by which to control the activities of the population, preventing people from engaging in peaceful demonstrations, from sharing news and information at sensitive times, and expressing their views.

Geotracking of Individual Locations

Several individuals described being arrested based on "geotracking" the locations of their mobile phones.[143] Geotracking can be done in several ways. Ethio Telecom's customer management system has location details of the mobile phone tower that is used for both caller and receiver for all past phone calls.[144] Mobile phones will utilize the strongest signal (usually meaning the closest mobile tower) to make calls. In Addis Ababa or other large cities where there is a greater density of mobile towers, knowing the location of the mobile tower that a call is made or received through could reveal someone's location to within 50 meters. In the more rural areas where there may be only one mobile tower, Ethio Telecom's geotracking capabilities provide less useful information about someone's location. Locations of phone calls are often revealed to detainees by security officials during interrogations. While many rural *kebele*s require written authorization, whether legal or not, for residents to visit neighboring *kebele*s, security officials' easy access to phone record location data gives officials a timeline of an individual's movements.

In other cases, individuals were arrested based on real-time geotracking of their current location. According to former Ethio Telecom employees, real-time monitoring of the location

---

[142] See UN HRC, Report of the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (hereinafter, "Report of the special rapporteur on the Internet"), U.N. Doc. A/HRC/para.49/50, May 16, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed February 12, 2014).

[143] Geotracking is the identification of a person's physical location by obtaining information from their telephones. In Ethiopia this is carried out by identifying tower location of dialed or received phone calls.

[144] This information is often collected as a normal part of billing processes. However, many telecom operators will delete this data after a prescribed time to protect the privacy of users.

of mobile phones can be carried out through the ZSmart system, which reveals location information (based on proximity to mobile towers), as long as a phone is turned on.

In many cases, however, individuals who were being monitored by security officials were arrested after a series of phone calls from phone numbers that individuals recognized as a security officer's. These officers had previously called and harassed these individuals so their numbers were known to them. The calls in quick succession would indicate where, in general terms, the targeted individual was (based on mobile tower location). In some cases, the security official would have a brief conversation, in other cases, they would simply hang up. After security had ascertained the target's approximate location, subsequent phone calls would be made to further refine the location and when security officials are nearby the moment the target picks up the phone this is seen by security and the target is arrested. On two occasions described to Human Rights Watch, this technique was revealed by security officials to the arrested target.[145] Individuals also told Human Rights Watch that leaders of the Muslim protests in 2012 and 2013 were arrested based on geotracking their mobile phone locations. These claims have not been corroborated.[146]

Human Rights Watch has found no evidence of any GPS capability or other more precise means of identifying mobile caller locations being used in Ethiopia, other than use of such mobile tower data.

Despite the availability of this technology, one regional police officer from eastern Oromia describes their unsophisticated, yet incredibly effective means of locating people:

> We often know the location of people because we have people at all levels from *kebele* to *woreda* to individual farms. We know everything. Nothing happens without someone knowing. But if we do not know where they are for some reason, we can call a special department at federal police with the phone number, they get in touch with Ethio Telecom and then we get that person's location. We don't need to use technologies very often, as we have such a closely connected network at all levels from household on up.

[145] Human Rights Watch interviews #80 and #89 (names and locations withheld), July 2013.
[146] Human Rights Watch interview #102 (name and location withheld), October 2013.

> We know every step, every movement. People only travel in groups—if they go as individuals they usually need some sort of paper, so we often don't need these technologies at our level. We know what people are saying and who they are speaking to. We can arrest anytime—we don't need any evidence.[147]

Controlling the Internet

Internet use is in its infancy in Ethiopia, particularly outside of Addis Ababa. Nonetheless, there is small but active community of online activists and the Internet is playing an increasingly important role in the spread of ideas, information, and perspectives among the young and educated. As is the case with the telephone system, Ethio Telecom is the sole Internet access provider and the government uses various means to keep access restricted, including by blocking websites, accessing individual email accounts, and intimidating users to censor their online content. The governmental also uses some of the world's most advanced surveillance software to target key individuals in the diaspora. Concerns about Internet controls seem likely to increase with Ethiopia's ambitious Internet expansion plans.

Internet Filtering

Ethiopia routinely blocks websites that are critical of the government. Opposition parties, diaspora media sites, blogs, and numerous human rights sites are blocked and completely unavailable in Ethiopia. In a country in which independent media is extremely limited, journalists are threatened and forced into censoring their writings, and both national and foreign reporters have been charged under the anti-terrorism law, access to independent websites that offer critical analysis and alternative perspectives is vital.

Ethiopia was the first sub-Saharan African country to begin blocking Internet sites.[148] The first reports of blocked websites appeared in May 2006 when opposition blogs were unavailable,[149] and blocking has become more regular and pervasive ever since. Human

---

[147] Human Rights Watch interview with former regional police official (name and location withheld), May 2013.

[148] Rebecca Wanjiku, "Study: Ethiopia only sub-Sahara Africa nation to filter Net," *InfoWorld*, October 8, 2009, http://www.infoworld.com/print/95151 (accessed April 7, 2013).

[149] Cathy Majtenyi, "Press Groups says Ethiopia Censors the Internet," Reporters Without Borders, May 24, 2006, http://www.voanews.com/content/a-13-2006-05-24-voa39/312751.html (accessed January 2013).

Rights Watch and the University of Toronto's Citizen Lab[150] conducted testing in-country in July and August of 2013 to assess the availability of 171 different URLs that had a higher likelihood of being blocked, based on past testing, on the Ethio Telecom network. A total of 19 tests were run over seven days to ensure reliability of results. Human Rights Watch

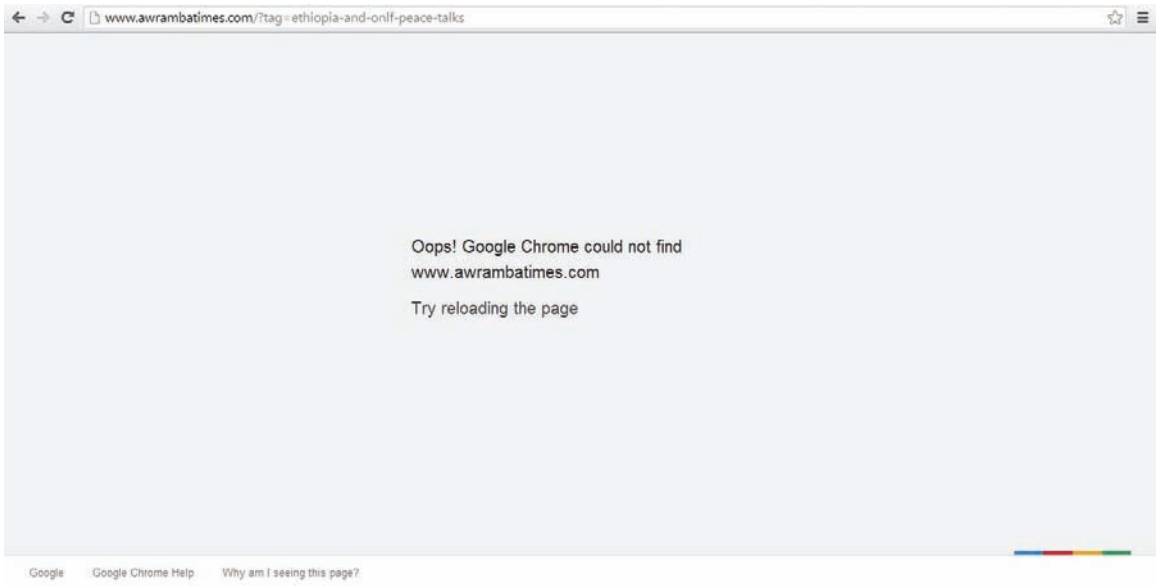


Figure 2. Awramba Times website error message when accessed in Ethiopia. Woubshet Taye, the former deputy editor of the Awramba Times is currently imprisoned in Ethiopia, convicted in January 2012 under the flawed anti-terrorism law.

conducted additional, ad hoc testing of select URLs in October 2013. The Open Network Initiative (ONI) previously conducted similar testing in 2007, 2009, and 2012.[151]

The vast majority of blocked sites are those that focus exclusively on Ethiopian content and are run by Ethiopian organizations or individuals (either in Ethiopia or in the diaspora). Human Rights Watch and Citizen Lab testing in Ethiopia shows that as of mid-2013, virtually all of the opposition websites, diaspora media (Ethiomedia, Goolgule, Ethiopian

[150] Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, Canada focusing on advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security.

[151] Prior testing revealed extensive filtering of political content in Ethiopia, with a "broad variety of political and news-related websites … blocked." OpenNet Initiative, "Update on information controls in Ethiopia," November 1, 2012, https://opennet.net/blog/2012/11/update-information-controls-ethiopia (accessed March 14, 2014); OpenNet Initiative, "Country Profiles: Ethiopia," September 30, 2009, https://opennet.net/research/profiles/ethiopia (accessed February 12, 2014. OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto, the Berkman Center for Internet & Society at Harvard University, and the SecDev Group.

Review, Nazret), and blogs that offer critical analysis of Ethiopian political affairs were blocked. Opposition websites that were blocked included those of banned organizations (such as Ginbot 7). The websites of journalists convicted under the anti-terrorism law have been blocked including Ethiomedia (managed by Elias Kifle) and ESAT.[152] Other Ethiopia-based media sites were blocked. Many blogs were also blocked—in 2012 Ethiopia reportedly blocked Google's Blogpost service, along with all blogs it hosted (Blogpost was a popular blog-hosting service in Ethiopia).[153] See Appendix 1 for a list of tested websites that were found to be blocked in the August 2013 testing.[154]

Of equal interest to what is blocked is what is not blocked. None of the websites of foreign NGOs working on Ethiopian issues are blocked in Ethiopia. Very few media outlets run by international organizations that cover Ethiopian affairs are blocked—notable exceptions are the news organizations Al Jazeera and Al Arabiya.[155] The Voice of America's website is freely available but their radio signals are routinely jammed. Gmail, Facebook, and Twitter are available although some individual Facebook groups are blocked (such as Addis Neger), particularly when accessed through unencrypted (http ://) channels.[156] Document sharing sites such as Google Docs or Dropbox are freely available. YouTube is also freely available although some specific videos are blocked.

Despite legislative prohibitions on use of Internet voice (VoIP) services, Skype's website is freely available. The Telecom Fraud Proclamation criminalizes the commercial provision and use of VoIP services. The government has stated that private Skype use is still permitted. In countries where nationwide filtering is in place, governments often seek to block adult sites, gambling sites, online dating sites, and sites promoting hate. ONI testing from 2012 reveals that none of the sites tested for in these categories as part of its

---

[152] See Human Rights Watch's publications on the Anti-Terrorism Proclamation at: http://www.hrw.org/africa/ethiopia/.

[153] Human Rights Watch interview with former blogger (name and location withheld), May 2013.

[154] The list of blocked websites in Appendix 1 is not comprehensive and only provides a sampling of the websites found to be blocked in 2013 testing. The absence of a website from the list of blocked URLs does not necessarily mean the site is accessible in Ethiopia. In addition, because the list of websites tested is not comprehensive, results may underestimate the extent of material that is blocked.

[155] Al Arabiya is a media outlet based in Saudi Arabia and owned by Saudis that provides English and Arabic language news and current events programming.

[156] Human Rights Watch interview with former blogger (name and location withheld), November 2012. Many of the Facebook groups that are unavailable through the unencrypted version are on different Ethiopian political movements, including *Bekaa* ("enough"), "Free Eskinder Nega," and various groups calling for "revolution."

methodology were blocked in Ethiopia. Human Rights Watch did not test sites in these categories during the 2013 testing.

Figure 3. Google Analytics data showing drop of Al Jazeera English traffic in Ethiopia after material was published that was critical of government's handling of the Muslim protests.

In May 2012, Al Jazeera's website and YouTube channel were briefly blocked following a documentary that was critical of Ethiopia's handling of the Muslim protests. On August 2, 2012, Al Jazeera's website was once again blocked the day an Al Jazeera program appeared online that was critical of Ethiopia's handling of Muslim issues.[157] Three days prior to the blocking, another article appeared on Al Jazeera about clashes in southern Ethiopia.[158] Data presented by Al Jazeera from Google Analytics[159] show that traffic from Ethiopia to Al Jazeera's English language website from dropped from 50,000 users in July 2012 to just 114 in September 2012. A similar drop occurred on its Arabic website.[160] Users in Ethiopia reported that the term "aljazeera" was not searchable on Google and only became available again in mid-March 2013.[161] Other individual programs have been blocked on

[157] Program can be seen at: "Aljazeera Mubasher TV channel Exposed the Interference of Ethiopian Govt. on Muslims religious matter and Discussed with the prominent guests on the current movement of Ethiopian Muslims," video report, *Al Jazeera*, August 2, 2012, http://www.youtube.com/watch?v=pJqXjJgoR4A&feature=youtu.be (accessed February 12, 2014). Article can be found at "Ethiopian journalists sentenced for 'terrorism,'" *Al Jazeera*, July 13, 2012 http://stream.aljazeera.com/story/ethiopian-journalists-sentenced-terrorism-0022284 (accessed February 12, 2014).

[158] Article can be found at: "Ethiopia erupts in deadly ethnic violence," *Al Jazeera*, July 31, 2012, http://www.aljazeera.com/news/africa/2012/07/201273075846287757.html (accessed January 12, 2014).

[159] Google Analytics is a service offered by Google that generates detailed statistics about a website's traffic and traffic sources.

[160] Analytics image from: "Ethiopia 'blocks' Al Jazeera websites," *Al Jazeera*, March 18, 2013, http://www.aljazeera.com/news/africa/2013/03/20133179361372518 2.html (accessed February 12, 2014).

[161] Email communication between blogger and Human Rights Watch, April 2013.

YouTube in Ethiopia, and the July 12, 2013 program on the Muslim protests was blocked on YouTube in Ethiopia as of October 2013.[162]

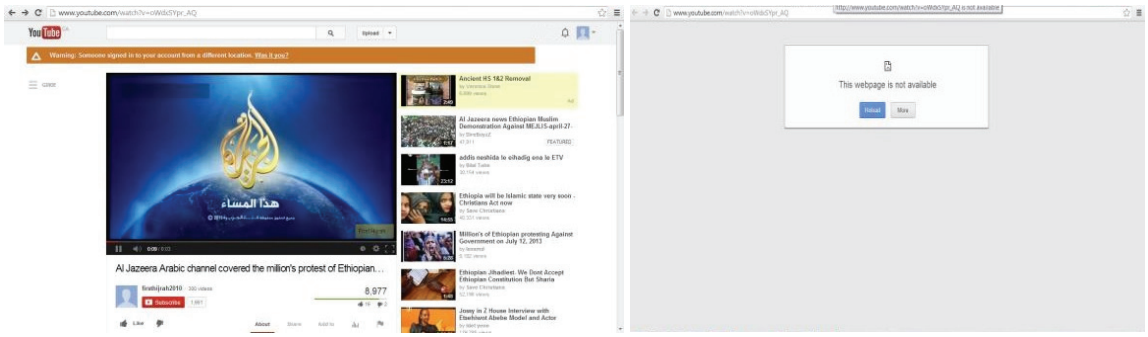


Figure 4. On the right is the error message users receive in Ethiopia in October 2013 when they try to access Al Jazeera Arabic's program that covered the Muslim protests in July 2013. On the left is the same Al Jazeera program accessed from outside of Ethiopia at: http://www.youtube.com/watch?v=oWdxSYpr_AQ.

The increased popularity of social media and the availability of video on mobile phones in Ethiopia resulted in several videos from the Muslim protests that show police using excessive force against protesters. These videos were immediately uploaded on YouTube and were almost immediately blocked in Ethiopia and remain so.[163]

While some websites like Al Jazeera are blocked for a limited period of time in response to specific events, most websites that are blocked seem to remain blocked.

Other key incidents show the sensitivity of the government to information that could prove embarrassing to the ruling party. On May 18, 2012, Abebe Gellaw garnered international attention when he orally criticized then-Prime Minister Meles Zenawi at the G8 summit in Washington DC. Any information on this incident, including the YouTube video of the incident, was immediately blocked in Ethiopia. Many people inside Ethiopia did not know about the incident until much later. As of September 2013, one of the YouTube videos of this incident had amassed almost 700,000 hits,[164] while in Ethiopia it was virtually unheard of. The video is still blocked in Ethiopia as of October 2013.[165] Numerous individuals told Human Rights

[162] Human Rights Watch Internet filtering testing, October 2013.

[163] Email communication between blogger and Human Rights Watch, April 2013.

[164] The most popular version of this video is available at: "ESAT News: Meles Zenawi humiliated in G8 meeting," video report, *ESATtv Ethiopia*, May 18, 2012, http://www.youtube.com/watch?v=hUVsq-FDFRE (accessed February 12, 2014).

[165] Human Rights Watch/Citizen Lab Internet filtering testing, October 2013.

Watch that the YouTube video of this event, blocked in Ethiopia, eventually ended up for sale on DVDs on street corners throughout Addis Ababa. This incident illustrates the control that Ethiopian authorities are able to exert over access to information through its control of the telecom system and its decimation of independent media. No Ethiopian media outlet dared report this incident, websites featuring the video were immediately blocked, and foreign TV and radio stations that would have covered the incident were jammed.

Users living in other countries, such as China and Iran, that implement nationwide filtering employ various tools to circumvent web filters and access blocked information. In Ethiopia, very few users circumvent web filters due to a lack of awareness of tools and methods, slow connection speeds, and the blocking of circumvention websites. Human Rights Watch and Citizen Lab testing revealed that the websites of circumvention tools Tor, Ultrasurf, and others were all blocked. ONI testing in 2012 also found these websites were blocked.

Various users in Ethiopia report that certain keywords—such as OLF and ONLF—do not appear on unencrypted versions of Google (http://) and other popular search engines. Switching to encrypted versions (https://) gets around this simple blocking of keywords. As of October 2013, major search engines were accessible in Ethiopia.[166]

Based on available testing information, Internet filtering appears to take place through several methods. In some cases, websites are blocked by domain name (example.com) or URL (http://example.com/specificpage). If a site is blocked by domain name, then all other sub-domains will also be blocked. For example, if blogspot.com (domain) is blocked (as it has been in previous testing in Ethiopia), then all blogs hosted on the service (exampleblog.blogspot.com) will also be blocked, leading to considerable blocking of innocuous content. Since Ethio Telecom is the sole Internet access provider and controls all Internet gateways that connect the country to the global Internet, domain name and URL blocking would be fairly straightforward to implement nationwide.

In addition, certain keywords present in a URL or search term, when detected, will trigger blocking in the form of a timeout or other browser error message if using a website that is not using or does not support encryption (http://). Globally, this method is relatively unique

[166] Ibid.

and is similar to the kind of keyword filtering long documented in China.[167] Such keyword filtering can be implemented through use of deep packet inspection (DPI), which is now confirmed to be in use in Ethiopia. Deep packet inspection enables the examination of the content of communications (an email or a website) as it is transmitted over an Internet network.[168] While some Internet access providers use limited DPI for commercial purposes, this technology can also be used to monitor Internet traffic on a nationwide scale and block specified content as data passes through the network. In May 2012, the Tor Project reported that DPI was being deployed in a way that could identify and block use of Tor in Ethiopia.[169] This would indicate a new level of sophistication and scale in use of DPI. Tor's finding followed a June 2011 tender issued by Ethio Telecom to acquire DPI.[170] In June 2012, then-Ethio Telecom CEO Jean-Michel Latute confirmed the use of DPI in Ethiopia.[171] However, Orange has told Human Rights Watch that it has not been involved in the selection and implementation of security equipment (like DPI) for the Internet in Ethiopia.[172]

Consistent with prior results in 2012, Human Rights Watch and Citizen Lab testing found that content is blocked through a particularly opaque method that makes it difficult for Ethiopian users to know whether lack of access is due to censorship or technical error.[173] When trying to reach a blocked site or if blocked keywords are detected, a user's browser will display an error message, for example, indicating that the connection has timed out. In

[167] OpenNet Initiative, "Country Profiles: China," August 9, 2012, https://opennet.net/research/profiles/china-including-hong-kong (accessed February 12, 2014).

[168] Once examined, the communications can be then copied, analyzed, blocked, or even altered.

[169] Runa Sandvik, "Ethiopia introduces Deep Packet Inspection," post to "Tor" (blog), Tor Project, May 31, 2012, https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection (accessed March 13, 2014). Previously, the method of blocking that Tor detected had only been used in a handful of states, including China, Iran, and Kazakhstan. The Tor project is a non-profit organization that conducts research and development into online privacy and anonymity, and offers a technology that helps protect privacy online. See Tor Project, "Tor: Overview," undated, https://www.torproject.org/about/overview.html.en (accessed March 14, 2014).

[170] Azi Ronen, "Ethio Telecom Issued a Tender for DPI," post to "Broadband Traffic Management" (blog), July 7, 2011, http://broabandtrafficmanagement.blogspot.com/2011/07/ethio-telecom-issued-tender-for-dpi.html (accessed March 14, 2014).

[171] "En Éthiopie, France Télécom accompagne la censure d'Internet," *La Croix,* October 6, 2012, http://www.la-croix.com/Actualite/Monde/En-Ethiopie-France-Telecom-accompagne-la-censure-d-Internet-_NP_-2012-06-10-816727 (accessed March 14, 2014). Jean-Michel Latute was on secondment from France Telecom. When France Telecom's contract with Ethio-Telecom was terminated in January 2013, he continued as CEO of Ethio Telecom for six more months.

[172] Letter from Brigitte Dumont, Chief Officer, Group Corporate Social Responsibility, Orange, to Human Rights Watch, November 19, 2013.

[173] For further technical explanation of the use of forged TCP RST (reset) packets to blocked online content, see OpenNet Initiative, "Update on information controls in Ethiopia," November 1, 2012, https://opennet.net/blog/2012/11/update-information-controls-ethiopia (accessed March 14, 2014).

other countries that filter the Internet, users will often see a page that explains that access to a site has been blocked pursuant to a particular law.

Internet Filtering Roles and Responsibilities

It is not clear who in the Ethiopian government provides direction on which websites to block. Based on interviews with numerous individuals from INSA and Ethio Telecom, it is likely that a variety of individuals and agencies have been involved in these decisions since filtering began in Ethiopia. However, all former intelligence and Ethio Telecom officials interviewed by Human Rights Watch suggested that the Ministry of Communications and Information Technology plays a key role. They believed that the blocking occurs with the use of Chinese technology and is done from within the Ethio Telecom offices.[174]

Internet filtering practices in Ethiopia do not appear to be regulated by law, nor subject to any kind of safeguard against improper or disproportionate censorship. As more and more Ethiopian citizens have the means to access the Internet, overbroad restrictions will limit its use as a valuable source of independent information and as a platform for communicating ideas and economic activity.

Email Monitoring and Forced Password Disclosure

In the vast majority of cases known to Human Rights Watch in which information derived from private emails has been used during interrogations or submitted as evidence in trials, the targeted individual was pressured to give up their email address and password. In some cases, interrogators knew the detainee's email address and used various forms of pressure to coerce them into giving up their password. Human Rights Watch found very few credible cases in which emails were used during interrogations or trials where the detainee did not provide their email password during interrogations. A former regional police commander in Oromia told Human Rights Watch:

> Passwords? We get passwords by force, no other methods. I don't know what happens at higher levels. There is no other way for us to get access to

[174] Human Rights Watch interviews with former government officials #8, 14, and 49, January 2013 and May 2013

> emails or Facebook. We always get passwords by force for those that are involved in politics, but we never even bother to do this for criminals.[175]

At the level of intelligence services, former Ethio Telecom and INSA officials described the use of various tools that would recover deleted email messages and instant messages (IMs) from Gmail, Yahoo Mail, and Hotmail accounts. Keywords could be searched for inside people's email accounts and Skype calls could be recorded and instant messaging monitored.[176]

Prior to 2012, access to email accounts required knowledge of the individual's email address and password, with the exception of passwords that were entered by users on the Woredanet, Schoolnet, and Agrinet systems.[177] Webmail and other passwords that were entered in these systems were available to INSA staff, easily facilitating access to email accounts of *woreda* employees, teachers, and other users of these donor-funded programs.

According to World Bank publications, the Bank was a funder of WoredaNet together with the African Development Bank through the Ministry of Capacity Building, and SchoolNet together with the UNDP.[178] International donors, including the World Bank, have an

---

[175] Human Rights Watch interview with former regional police official, (location withheld), May 2013.

[176] Human Rights Watch interview with former government official #49, (location withheld), May 2013.

[177] Human Rights Watch interview with former government employee #100, (location withheld), October 2013. Schoolnet is managed by the Ministry of Education and connects 550 high schools around Ethiopia with VSAT-based broadband Internet access for the purposes of video-based distance and standardized education. Agrinet was intended to connect 26 agricultural research institutions across Ethiopia with broadband Internet connections.

[178] World Bank, "World Bank Provides US$50 Million for Public Service Delivery Improvement, Citizen Empowerment, and Good Governance Promotion in Ethiopia," March 23, 2010, http://go.worldbank.org/VLCH71LCP0 (accessed March 19, 2014); Harry Hare, "Survey of ICT in Education in Ethiopia," infoDev/World Bank, 2007, http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/12/000333038_20081112230415/Rendered/PDF/463910BRI0Box31ia010ICTedoSurvey111.pdf (accessed November 8, 2013). MCIT states on its website, "The EICTDA, through funding from the World Bank, was able to launch a series of projects that improved ICT access in the public sector. It commissioned a series of studies on IT standards and frameworks. These range from technical standards on selection of hardware and software, to e-government Interoperability framework, to E-service standards. The EICTDA was also able to draft laws governing the online environment including e-commerce law, data protection law and digital signature law." MCIT, "ICT Policy and Regulatory Environment," undated, http://www.mcit.gov.et/web/english/ict-policy-and-regulatory-environment (accessed March 19, 2014). See also, World Bank, "Additional Financing to the Public Sector Capacity Building Program Support Project," 2010, http://www.worldbank.org/projects/P107217/public-sector-capacity-building-program-support-project?lang=en (accessed March 19, 2014); World Bank, "ICT Assisted Development Project: Updated Project Information Document (PID)," Report No: AB135, April 9, 2004, http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2004/04/14/000104615_20040414094134/Rendered/PDF/PIDoPo78458.pdf (accessed March 19, 2014); MCIT, "The National ICT for Development (ICT4D) Five Years Action Plan for Ethiopia [2006 – 2010]," May 2006, http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan040825.pdf

important role to play in enhancing people's Internet and telephone access. However, when financing such projects in Ethiopia, donors need to ensure they are undertaking proper due diligence to ensure that they are not directly or indirectly financing censorship, Internet filtering, illegal surveillance, or network shutdowns. The World Bank and other donors should also assess the risks to privacy, freedom of expression, association, and movement, and access to information of its projects with ICT components prior to project approval and throughout the life of the project. They should identify measures to avoid or mitigate these risks and comprehensively supervise the projects, including through third parties.

The extent and capabilities to intercept Internet traffic and monitor online communications are unknown and difficult to determine. Despite the use of unsophisticated techniques such as forced password disclosure, and email monitoring not yet being a commonly used intelligence gathering technique in Ethiopia, there is increasing evidence that the Ethiopian government has recently acquired advanced technologies to monitor the email and online behavior of targeted individuals since 2012.

One former official described printout of intercepted materials in INSA's office bearing the logo of ZTE's ZXMT centralized monitoring system. According to several sources, ZTE employees located in the Ethio Telecom building provide technical support to both ZSmart and to this surveillance technology.

ZTE highlights its ability to centralize the monitoring of communications across different kinds of networks and products, including wired phone lines, mobile, and the Internet. ZXMT also utilizes deep packet inspection to scan all Internet traffic flowing across a network. Researchers analyzing the deployment of ZXMT in Libya found that the system appears capable of intercepting web-based email, email accessed via client software (like Outlook), web browsing, and chat.[179] The systems and capabilities of technologies described by former officials mirror the surveillance capabilities of ZTE's ZXMT interception system.

(accessed March 19, 2014), p. 15; Aman Assefa, "ICT in Ethiopia: Challenges and Prospects from an A2K Perspective World Bank," 2009, http://www.law.yale.edu/images/ISP/A2KGA_Proceedings.pdf (accessed March 19, 2014).

[179] John Scott-Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution* (Newport, RI: US Naval War College, Center on Irregular Warfare and Armed Groups, 2013).

Evidence exists that this cutting-edge surveillance system was used in both Libya and Iran.[180] In a 91-page promotional document called "Talking to the future" presented to the Iran Telecommunications Research Center, ZTE describes the system as their "turn-key, carrier-class lawful interception solution," a "vendor-independent" monitoring system with "powerful interoperability."[181] ZTE noted that its ZXMT system was applicable to military and national security agencies.[182] ZTE described the advantages of its ZXMT's lawful interception system: it can be integrated with common telecom services, has high security and good secrecy, and has powerful multiservice monitoring ability. It also suggested the system is "invisible to the targets."[183]

Human Rights Watch wrote to ZTE to verify the sale of ZXMT to Ethio Telecom or Ethiopian authorities, and to inquire about ZTE's role in implementing or providing training and support for lawful intercept, network filtering and management, or DPI systems in Ethiopia. We also asked about ZTE's approach to human rights due diligence and any human rights policies it has in place to prevent abuse of its technologies. ZTE did not respond to our letter or follow-up email, other than to acknowledge receipt.

Human Rights Watch has been unable to verify whether ZXMT systems are sold by ZTE directly or via one of its subsidiaries. In September 2012, ZTE sold its subsidiary ZTE Special Equipment Company (ZTEsec), which marketed Internet network interception and monitoring technology (including DPI solutions).[184] ZTEsec now operates as Sinovatio. Human Rights Watch also wrote to Sinovatio to inquire about any role it played in selling, implementing, or providing training and support for surveillance technologies in Ethiopia.

---

[180] See "PSTN Transformation Via ZTE NGN Solution," ZTE presentation to the Iran Telecommunications Center, May 2008, on file with Human Rights Watch and John Scott-Railton, *Revolutionary Risks*.

[181] "PSTN Transformation Via ZTE NGN Solution," ZTE presentation to the Iran Telecommunications Center, May 2008, on file with Human Rights Watch.

[182] Steve Stecklow, "Special Report: Chinese Firm helps Iran spy on citizens," *Reuters*, March 22, 2012, http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322 (accessed March 14, 2013).

[183] "PSTN Transformation Via ZTE NGN Solution," ZTE presentation to the Iran Telecommunications Center, May 2008, on file with Human Rights Watch.

[184] ZTE Corporation, "Announcement: Disposal of Equity Interests in Shenzhen ZTE Special Equipment Company Limited," September 21, 2012. See also, Sinovatio, "Welcome to Sinovatio Technology," undated, http://www.sinovatio.com/en/about/introduction.shtml, (accessed December 5, 2013).

Sinovatio acknowledged receipt of our letter, but did not respond substantively to our letter or follow-up email.[185]

Eric King of Privacy International, one of the world's leading researchers on surveillance technology, told Human Rights Watch that, "one of the things that sets ZTE apart is that when it enters a telecom market it often packages all of its products together as part of its contract, so you get the 'lawful' interception products unless you specifically request to opt out of it. Not too many governments that ZTE does business with are likely to do this."[186] Though not conclusive, the evidence suggests that Ethiopia has acquired and is using the ZXMT interception system.

Ethiopia's country code top-level domain suffix is ".et" and Ethio Telecom's exclusive control over the .et email and .et top-level domain provides the government with virtually unlimited access to all .et emails. All .et email passwords are included in ZSmart's customer information profiles enabling easy access for Ethio Telecom employees. Use of .et email addresses is not widely used in Ethiopia because of service interruptions and the perception of pervasive surveillance, with even senior government officials preferring to use more popular web-based email services.

Human Rights Watch received several accounts of individuals who were arrested for involvement in politics and shown their emails and Facebook posts during interrogations. However, in each of these cases they were either pressured into revealing their email addresses or passwords, or practiced very poor digital security (for example, not logging off of email at Internet cafes, not adjusting privacy settings on Facebook, etc.). In none of these cases was there clear evidence of any use of the more sophisticated surveillance technologies described.

[185] Human Rights Watch received an email in response to our letter, but the email was blank and contained no substantive response to our inquiry.

[186] Human Rights Watch interview with Eric King, Privacy International, London UK, February 2013. The term "lawful intercept" is used by equipment makers as an industry label for systems that enable surveillance. However, the term does not necessarily mean surveillance practices are legal under national or international law.

One man from Wollega, now resident in Kenya, described how his friends were arrested because of a group Facebook chat among himself and three friends. It is not known how his Facebook information was accessed. He said:

> They arrested all four of the people in the chat except me as I was already here [Kenya]. They were part of the local Oromo Youth Association. They were pressured into giving their passwords after their arrest…. They were all jailed together, and then one by one were taken out of cell and beaten or threatened into giving up their passwords and then were sat in front of the computer while the security people went through their emails—"Who is this person? What do they do?"… If they are Oromo names and they live outside of the country and they do not know who they are then they consider them to be OLF. If they are Amharic names from the outside, then they are considered to be Ginbot 7. They were forced to sign a form that they would not chat with individuals outside of the country and would not engage in any community mobilization or politics. They also have to report to police every Friday. All of our chats involved using code words so it is not always obvious what is being spoken about…. This happens everywhere and all the time now. It is nothing new. We have these new technologies but now we are fearing to use email and Facebook.[187]

An Oromo woman who was detained twice in military barracks in Eastern Oromia for speaking out publicly against the government described her final interrogation based on the content of her phone calls, email, and Facebook posts. She accessed her email through a computer connected to Woredanet:

> They [security] detained me: They took my phone when arrested and went through the contacts: "All of these numbers are from Arab countries; you are communicating with them about religious issues and are causing problems." They told me it was forbidden to post anything about religion on Facebook or to have a religious ringtone on the phone that I had. "You are behind the Arab uprising, you were calling them, you are posting religious

[187] Human Rights Watch interview #31 (name and location withheld), May 2013.

> messages on Facebook." They asked me in detail what I was speaking about during my phone calls. "We have your voice recorded. You are lying." They didn't present these recordings but showed me printed emails [written in Afan Oromo] that I had sent. They selected some emails and asked me about them. They were about religious issues, human rights issues, etc. Also some of my Facebook posts discussed these issues. They played one recording of a phone call I had with family members in Saudi Arabia.[188]

Despite the availability of technologies to access individual email accounts, very little evidence exists yet of this potential being utilized in Ethiopia beyond a few cases.

Restricting Access to the Internet

Access to the Internet is easily controlled if a government controls all the Internet service providers in a country—as is the case in Ethiopia. Many Ethiopians, particularly outside of Addis Ababa, access Facebook and email on their mobile phones given the lack of Internet cafes in rural areas, lack of privately-owned computers, and the availability and cost of private Internet connections. Preventing access to mobile phones through blocking of SIM cards and refusal of SIM card sales to blacklisted individuals results in an inability to access the Internet.

One of the documented techniques that Ethiopian security officials have used in the past to control dissenting individuals is to restrict movement of individuals upon their release from detention, often requiring them to sign letters that state they will not move outside of a certain location and often requiring daily or weekly check-ins at the local police station to ensure that movements are restricted. One individual described being arrested several times and accused of writing emails to "mobilize students for the OLF." He was never charged. Upon his last release he was forced to sign a letter that stated because he had used email to mobilize for the OLF, he would not go to Dire Dawa—the nearest town with an Internet café—to access the Internet. He was required to check in with the authorities weekly.[189]

---

[188] Human Rights Watch interview #86 (name and location withheld), July 2013.

[189] Human Rights Watch interview #63 (name and location withheld), July 2013.

Many individuals reported that once there was any sign that they or their accounts were under surveillance they stopped using their email accounts altogether.

Internet Cafes: Rules for Cafe Operators

Many urban Ethiopians access Internet and email through the increasingly ubiquitous Internet café. Policies and procedures governing Internet cafes are not transparent and different café operators are under varying levels of pressure from security officials. One café operator told Human Rights Watch he was told by a security official that all computer screens must be physically positioned so as to be visible to the café operator and that he must report any "unusual behavior" to security officials.[190] Another described being threatened with having her equipment confiscated because users were accessing content that was critical of the government. She said she was threatened by security officials with five years' imprisonment if it happened again.[191] It is not known whether users were accessing unblocked websites or whether the café owner was helping them use a circumvention tool to get around web filtering.

There have been various efforts in the past to regulate Internet café use and different reports have suggested that as of 2006 users must provide name and identification.[192] While presently some cafes require users to log their name and identification details, in practice this is not done with any consistency.

One cafe operator reported being fearful whenever anyone would try to use Tor or any other circumvention tool because of fear of reprisals from government.[193] A frequent café user told Human Rights Watch it is not common for café operators to assist users to use Tor or other circumvention tools. Café employees report frequent visits from security officials sometimes asking questions about specific users and what they accessed, while at other times asking general questions about suspicious behavior. Some users told Human Rights Watch that some café employees express frustration when users delete their browsing history, afraid of not being able to answer questions about user behavior during the regular visits of security

---

[190] Human Rights Watch interview #9 (name and location withheld), January 2013.

[191] Human Rights Watch interview #13 (name and location withheld), February 2013.

[192] Groum Abate, "Ethiopia Internet cafes start registering users," *Capital*, December 27, 2006, http://nazret.com/blog/index.php/2006/12/27/ethiopia_internet_cafes_start_registerin (accessed March 14, 2014).

[193] Human Rights Watch interview #46 (name and location withheld), May 2013.

officials. A café operator in Addis Ababa said he believed that most of the surveillance done in cafes was carried out by plainclothes security officials or café workers physically watching users' computer screens to see what people were doing online.

Pressure to Censor: Threats to Bloggers and Facebook Users

Human Rights Watch did not find any cases in which individuals were targeted because of what they accessed online, but there are numerous instances where individuals were targeted for what they posted online through blogs or Facebook.

While blogging is very much in its infancy in Ethiopia, the blogging community is increasing in size and critical writings appear with more frequency. With the growth in blogging over time in Ethiopia, many bloggers have been under pressure from the government to censor their writings. Since 2009, many blogs in Ethiopia (see Appendix 1) have been blocked and many bloggers stopped writing after their blogs were blocked.

Many others have experienced pressure to censor their postings on Facebook and other public forums. Sometimes this takes the form of threatening messages on Facebook from unknown people who do not identify themselves, while other times security personnel visit or phone the individual and threaten or pressure them to stop posting certain photos or articles, particularly on Facebook. This suggests ongoing monitoring of Facebook users. Such monitoring could occur through a number of methods, from simply observing public Facebook activity to creating fake accounts to befriend targets, compromising account passwords, or intercepting unencrypted Facebook traffic.

Adjusting privacy settings on Facebook would provide some level of protection from harassment, but awareness in Ethiopia about these settings is quite low. Facebook is also one of the few mediums where Ethiopians express themselves quite openly. Anecdotally, it does not appear to be used to organize meetings and gatherings the way it has been used in other countries. One user said: "I think there is a perception [in Ethiopia] that Facebook in anonymous. Because Facebook use is relatively new in Ethiopia, government officials have not seen the role it can play in spreading ideas that otherwise cannot be spread. They are more concerned with the formation of social

movements that Facebook was used for in Egypt and elsewhere. In Ethiopia Facebook is not used for that."[194]

Nonetheless, more and more people are having problems because of what they publicly post on Facebook. One person described being harassed because of having posted an OLF flag on their Facebook account:

> My problems started in August 2012. Before 2012 I had been suspected of being OLF. When the prime minister [Meles Zenawi] died I was ordered to collect money in his memory though I complained about having to do it. Security services said they saw the OLF flag on my Facebook page. They chat with people on Facebook. If someone uses it in rural areas, security follows those Facebook users. "We see what you are posting [on Facebook]."[195]

Other individuals told Human Rights Watch being forced to change their Facebook postings because they posted materials about banned organizations, religious issues, were critical of the late Prime Minister Meles Zenawi, or posted material from blocked websites.[196]

Another individual described the pressure he was under to censor his blogs that satirized politics and current events. Three plainclothes security officers came to his compound in Oromia in early 2012 and threatened him for what he wrote on Facebook. His blog has also been blocked on at least six different occasions. He stopped blogging altogether for several months. He has resumed blogging but is now "very careful about what I say."[197]

As Facebook and blogging becomes more popular in Ethiopia, Facebook users and bloggers are coming under increased pressure. Human Rights Watch is not aware of users of other online services being under pressure to censor their content.

---

[194] Human Rights Watch interview #93 (name and location withheld), July 2013.

[195] Human Rights Watch interview #94 (name and location withheld), July 2013.

[196] Human Rights Watch interviews with various Facebook users.

[197] Human Rights Watch interview #61 (name withheld), November 2012 and email communication between blogger and Human Rights Watch, (date withheld).

Major Internet Companies in Ethiopia: Transparency Reports

Given concerns over privacy of user data, since 2012 a number of Internet companies have made aggregated data available on national government's requests for user data and the results of those requests. According to the reports of Google, Facebook, Microsoft, and Twitter, Ethiopia has not made any requests for user data or has made so few requests that they are not listed in the report.[198] By way of comparison, in the first half of 2013, Egypt had made 8 requests, and the UK made 2,337 requests for user data to Facebook, though each country has far more Internet users than Ethiopia. In general, sub-Saharan African countries are making very few user requests. Only three sub-Saharan African countries made requests for user data to Facebook during the first half of 2013.[199] According to Google, Ethiopia has not made a single request for user data since July 1, 2009, though Google does not report this data if there were less than 30 requests in the reporting period.[200]

New Technologies and Their Potential: Intrusive Malware

Many of the surveillance methods described in this report are mostly effective at targeting individuals physically located in Ethiopia. However, the government may have acquired powerful surveillance technologies that can be used to invade the privacy of individuals outside the country.

---

[198] Facebook transparency request reports can be found at: Facebook, "Global Government Requests Report," June 30, 2013, https://www.facebook.com/about/government_requests (accessed March 17, 2014). Facebook information was for the first half of 2013. Google's transparency reports for Ethiopia can be found at: Google, "Transparency Report," undated, http://www.google.com/transparencyreport/traffic/?r=ET&l=EVERYTHING&csd=1294957800000&ced=1297377000000 (accessed March 17, 2014), while Microsoft's is at: Microsoft, "Law Enforcement Requests Report," March 2014, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (accessed March 17, 2014). Twitter's transparency reports can be found at: Twitter, "Transparency Report," December 31, 2013, https://transparency.twitter.com/ (accessed March 17, 2014).

[199] Botswana, South Africa and Uganda were the three sub-Saharan countries. Facebook, "Global Government Requests Report," June 30, 2013, https://www.facebook.com/about/government_requests (accessed March 17, 2014).

[200] Google also only reports on data requests for law enforcement purposes, and often excludes national security related data requests. Data on data requests for law enforcement purposes is not available prior to July 1, 2009. Google, "Transparency Report," undated, http://www.google.com/transparencyreport/traffic/?r=ET&l=EVERYTHING&csd=1294957800000&ced=1297377000000 (accessed March 17, 2014).

Gamma and FinFisher

In August 2012, two groups of security researchers discovered the presence of a FinSpy "command and control" server in Ethiopia.[201] FinSpy is a surveillance system offered as part of a suite of governmental intrusion and remote monitoring solutions known as FinFisher.[202] At the time, Gamma International, a UK-headquartered company, sold FinFisher, along with training and other services, exclusively to governments.[203] Law enforcement and intelligence agencies are their primary customers. In October 2013, Gamma's FinFisher business became an independent company (FinFisher GmbH) headquartered in Germany.[204]

FinSpy is a type of remote monitoring tool (often referred to as spyware or malware) that can be surreptitiously installed on a target's computer. A common method is to send an email that contains a malicious link or file disguised as a legitimate item of interest to the targeted individual. If the target clicks on the link or opens the file, FinSpy installs itself onto the computer.

According to promotional materials, once installed, FinSpy can capture Skype communications, email, and chat conversations, collect passwords, and log all keystrokes.[205] The malware can also turn on the microphone or camera for live surveillance and extract or alter files stored on the hard drive. FinSpy sends any collected information back to the command and control server operated by the government agency that purchased the software. Finally, FinSpy is designed to be covert and undetectable by the user and commercial anti-virus software.[206]

---

[201] Claudio Guarnieri, "Analysis of the FinFisher Lawful Interception Malware," post to "Security Street Rapid7" (blog), August 8, 2012, https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher (accessed March 17, 2014); Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri, "The SmartPhone Who Loved Me: FinFisher Goes Mobile?" Citizen Lab, Research Brief No. 11, August 2012, https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/ (accessed March 17, 2014).

[202] Gamma Group, "FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions," undated, http://wikileaks.org/spyfiles/docs/gamma/298_finfisher-governmental-it-intrusion-and-remote-monitoring.html (accessed March 17, 2014).

[203] Gamma International is part of the Gamma Group of companies. "Company Profile," Gamma Group, https://www.gammagroup.com/companyprofile.aspx (accessed September 3, 2013).

[204] FinFisher, "FinFisher: Company Profile," undated, http://www.finfisher.com/FinFisher/company_profile.html (accessed March 17, 2014).

[205] Gamma Group, "Remote Monitoring & Infection Solutions: FinSpy," undated, http://wikileaks.org/spyfiles/docs/gamma/289_remote-monitoring-and-infection-solutions-finspy.html (accessed March 17, 2014).

[206] Ibid.

The presence of a command and control server in Ethiopia, by itself, does not mean that the government is deploying FinFisher. However, given the high costs of these tools and the fact that Gamma states it only sells to governments, it is unlikely that a nongovernmental party would have purchased and used the tool in Ethiopia. Also, given how slow and unpredictable networks in Ethiopia can be, it is also unlikely that a third-party government would have located a server on Ethio Telecom networks.

However, in early 2013, researchers at the Citizen Lab identified and analyzed a FinSpy sample that communicated with an active command and control server in Ethiopia.[207] This sample was embedded in a photo that contained images of members of Ginbot 7, strongly suggesting that the government might be using FinSpy to target opposition group members overseas.

Researchers at Citizen Lab have not confirmed whether this particular image had been successfully used to install FinSpy onto a target's computer. However, subsequent testing by Citizen Lab, Electronic Frontier Foundation, and Privacy International identified three computers owned by members of the Ethiopian diaspora that were infected with FinSpy, or were targets of infection attempts.

In the first case, the owner of the infected computer, Tadesse Kersmo, is an Ethiopian national and member of the executive committee of Ginbot 7 residing in the UK, along with his wife. His wife was elected to the Addis Ababa city council in 2005 for the Coalition for Unity and Democracy opposition party. He describes how they were then constantly harassed, threatened, and occasionally detained until they emigrated in 2009 and were granted asylum in the UK. He was also told by an employee of Ethio Telecom that his phone was being monitored. He told Human Rights Watch of his fears upon learning that one of his laptops was infected with intrusive surveillance software:

> I use the computer and Internet a great deal both socially, academically, and for political activities. I have very real concerns about the Ethiopian regime having unfettered access to my computer, reading my emails and

[207] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, Research Brief No. 15, March 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ (accessed March 17, 2014).

> monitoring my calls. This is not only a gross invasion of my privacy, but I am also concerned that it could put myself, my wife, and other members of the political opposition in danger from the Ethiopian authorities…. I found it very disturbing that I was spied on through this medium…. I remain concerned even while I am away from Ethiopia that further attempts will be made to infect my computer.[208]

One of the group conversations that he had on Skype with Ginbot 7 leaders during the time of his infection ended up appearing on pro-government websites on June 20, 2013.[209] In February 2014, Privacy International brought a case on behalf of Tadesse in the UK, asking the UK National Crime Unit to investigate potentially unlawful interceptions of his communications, as well as the responsibility of Gamma in assisting any possible offenses.[210]

A second case involved the attempted infection in June 2012 of Yohannes Alemu, a member of Ginbot 7, currently based in Norway. In June 2012, his wife was harassed and interrogated by security officials about his political activities during a visit to Ethiopia. During her 20 days in Ethiopia, security officials were in contact with Yohannes by telephone and email and demanded that he provide contact information (names, email addresses, Skype addresses, etc.) for key Ginbot 7 members and other information about the operations of Ginbot 7. These instructions were contained in an email dated June 29, 2012. He did not respond, and received a follow up email the next day from the same pseudonymous Gmail address threatening his family.[211] Several days later, his wife was released and returned to Norway.[212] On August 2, 2012 he received his final email from this

---

[208] Human Rights Watch interview with Tadesse Kersmo, (location withheld), November 2013.

[209] See "Berhanu Nega receives half a million 'grant' from Egypt to run Ginbot 7 and ESAT (Audio)," *Awramba Times*, June 20, 2013, http://www.awrambatimes.com/?p=8639 or http://hornaffairs.com/en/2013/06/20/leaked-audio-eritrea-funds-esat-berhanu-nega/ (accessed March 17, 2014). This recording was leaked the same day Dr. Berhanu Nega testified in front of the United States Congress Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations.

[210] See Alinda Vermeer, "Explained: Our criminal complaint on behalf of Tadesse Kersmo," Privacy International, February 21, 2014, https://www.privacyinternational.org/blog/explained-our-criminal-complaint-on-behalf-of-tadesse-kersmo (accessed March 17, 2014).

[211] The email read: "I am waiting for your reply. I do not think you have the luxury of time. If you try to play dirty game, it will have a far reaching consequence to you and your family. You have a very stark choice. I need your reply within the next 12 hours." Email from (name withheld) to Yohannes Alemu, June 30, 2013. On file with Human Rights Watch.

[212] Human Rights Watch interview with Yohannes Alemu, (location withheld), February 2014.

email address, with an attachment he was asked to read.[213] He forwarded these emails to individuals inside Norway and to several other individuals in the Ethiopian diaspora. Subsequent analysis by Citizen Lab found that the attachment to this email was infected with FinFisher.

In a third case, the owner of the infected computer is a US citizen who has provided technical support to Ethiopian diaspora groups, including Ginbot 7, for the past few years under the pseudonym, "Kidane."[214] Kidane's computer was infected in October 2012, when he was forwarded the August 2, 2012 email from Yohannes (containing an infected attachment) for investigation. Upon opening the attachment to investigate, Kidane's computer was infected. While Kidane was not the original target of the email, the infection remained live for four-and-a-half months. During this time, FinSpy recorded Kidane's Skype calls, emails, and web searches.[215] Kidane resides in the US and is now bringing legal action against the Ethiopian government for violations of US wiretap and privacy laws.[216]

Human Rights Watch wrote to Gamma and recently-formed FinFisher to confirm the sale of FinSpy to Ethiopian authorities and inquire about their policies to address human rights harm, but received no response. It is unclear whether Gamma or FinFisher have human rights policies in place to respect rights.

In response to Citizen Lab research and inquiry about the government's use of FinSpy, an Ethiopian government spokesperson said in a statement to media, "I cannot tell you what type of instruments we're going to use or not. I've no idea, and even if I did, I wouldn't talk to you about it."[217] Human Rights Watch has written to the government to confirm and received no response.

Researchers at Citizen Lab have identified FinFisher command and control servers in over 30 countries and have analyzed malware samples that appear to target users in Vietnam

---

[213] Email on file with Human Rights Watch.

[214] *Kidane v. Ethiopia*, US District Court for the District of Columbia, Complaint, February 13, 2014, https://www.eff.org/document/complaint-32 (accessed March 14, 2014). Kidane states that he is not a member of Ginbot7.

[215] *Kidane v. Ethiopia*, Complaint.

[216] Ibid.

[217] Vernon Silver, "Gamma FinSpy Surveillance Servers in 25 Countries," *Bloomberg*, March 13, 2013, http://www.bloomberg.com/news/2013-03-13/gamma-finspy-surveillance-servers-in-25-countries.html.

and Malaysia.[218] A group of NGOs have filed a complaint at the Organisation for Economic Co-operation and Development (OECD) alleging that FinFisher has been deployed to target activists in Bahrain.[219] In response to initial reports of use of FinFisher in Bahrain in 2012, Gamma has denied that it sold FinFisher to the government, stating that the deployments may be using stolen demonstration versions of the software.[220]

Hacking Team

Hacking Team is an Italy-based company that develops and sells self-described "offensive" surveillance and hacking technology.[221] With offices in Milan, Washington, DC, and Singapore, Hacking Team offers a product called Remote Control System, which marketing materials describe as "eavesdropping software" that "hides itself inside target devices" and "enables both active data monitoring and process control."[222] Hacking Team promotes the product as a "solution designed to evade encryption" that can be installed remotely, which allows the government to take control over the infected computer or mobile phone.[223] The software can be used to monitor "from a few and up to hundreds of thousands of targets," managed through a "single easy to use interface."[224]

Once installed on a target's device, the software allows a government to: copy files; capture passwords typed into the device; record Skype calls; monitor chat, email, and web browsing; and activate the computer's camera or microphone to spy on the user.[225] Remote

---

[218] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, April 30, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/ (accessed March 17, 2014).

[219] Privacy International, European Center for Constitutional and Human Rights, Reporters Without Borders, Bahrain Center for Human Rights, and Bahrain Watch "OECD Complaint against Gamma International for Possible Violations of the OECD Guidelines for Multinational Enterprises," February 1, 2013, https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/jr_bundle_part_2_of_2.pdf (accessed March 17, 2014).

[220] Vernon Silver, "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy," *Bloomberg,* July 27, 2012, http://www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html (accessed March 14, 2014).

[221] Hacking Team, "Hacking Team: About Us," undated, http://hackingteam.it/index.php/about-us (accessed March 14, 2014).

[222] Hacking Team, "Remote Control System: Cyber intelligence made easy," undated, http://wikileaks.org/spyfiles/docs/hackingteam/147_remote-control-system.html (accessed March 14, 2014).

[223] D. Vincenzetti and V. Bedeschi, "Hacking Team: Remote Control System V5.1," undated, http://wikileaks.org/spyfiles/docs/hackingteam/31_remote-control-system-v5-1.html (accessed March 14, 2014).

[224] Hacking Team, "Remote Control System: Cyber intelligence made easy."

[225] D. Vincenzetti and V. Bedeschi, "Hacking Team: Remote Control System V5.1."

Control System is designed to be invisible to the user and undetectable by commercial anti-virus software.[226]

On December 20, 2013, a third party made three separate attempts to target two Ethiopian Satellite Television Service (ESAT) employees residing outside of Ethiopia with spyware through Skype.[227] ESAT is an independent, diaspora-run satellite television station. In each attempt, ESAT employees received a file through Skype from a known contact. The ESAT employees did not open the files, which were presented as and appeared to be a Word document or PDF file. However, if the employees had opened them, the files would have covertly downloaded or installed a program onto their computers. Testing by researchers at Citizen Lab found that the program appeared to be spyware that matched previously-established characteristics of Hacking Team's Remote Control System.[228] Citizen Lab researchers also determined that the program communicated with a remote server that also appears to be linked to Hacking Team.[229]

According to ESAT employees, the Skype account used to send the files belongs to a known contact that had previously collaborated with ESAT, but who had "disappeared for a while."[230] It is unclear who was controlling the Skype account when the attempts occurred.

In two of the attempts, the third party who targeted the ESAT employees claimed the file was an article of interest to ESAT, though the file displayed no text when opened. The third party encouraged the targets to open the files, insisting that the files had "worked fine" for him or her. In the third attempt, the file contained a copy of an article from ECAD Forum, an Ethiopian media website.

---

[226] Ibid.

[227] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/ (accessed March 13, 2014).

[228] Ibid.

[229] Ibid.

[230] Ibid.

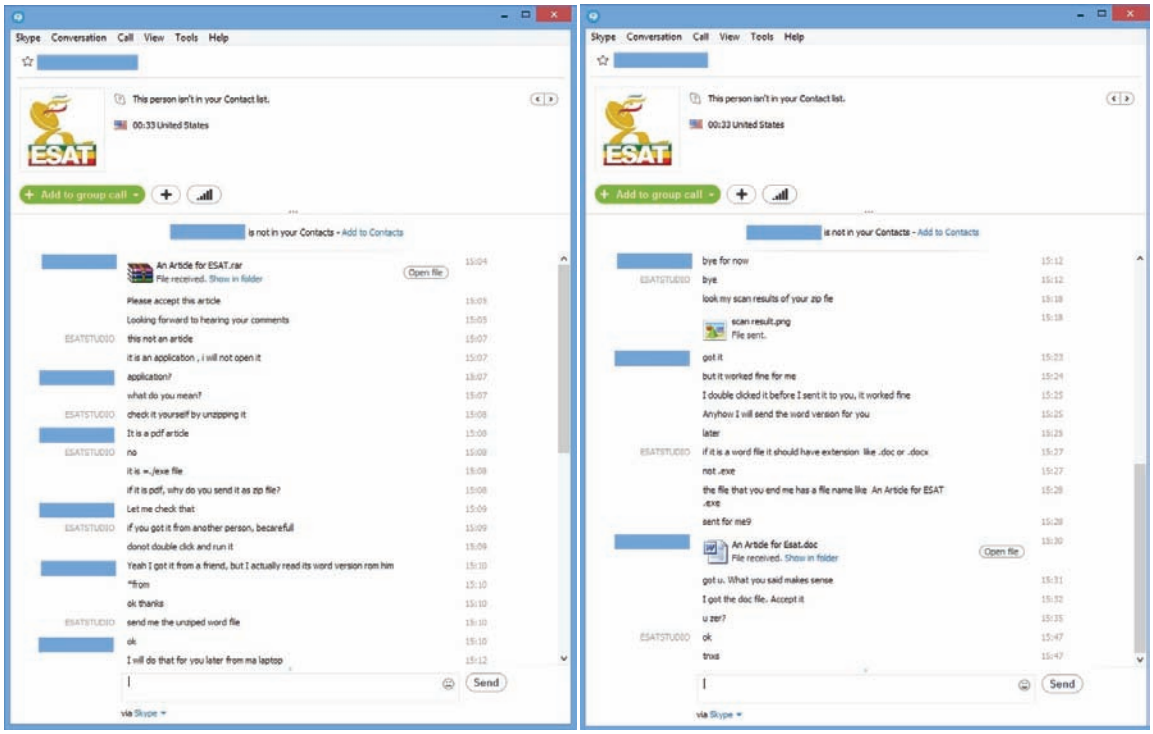


Figure 5. Screenshots of a file sent via Skype to ESAT employees on December 20, 2013. The ESAT employees did not open the files, but if they had, spyware that matched previously-established characteristics of Hacking Team's Remote Control System would have been downloaded onto their computers.

Hacking Team states that it sells exclusively to governments, particularly law enforcement or intelligence agencies, and not individuals or private businesses.[231] According to a Hacking Team spokesperson Eric Rabe, its products cost "hundreds of thousands of [US] dollars" and are customized for each client, based on their needs and local law.[232] The features that are enabled in a specific sale are based on a joint decision with the client, following a consultation.[233]

[231] Hacking Team, "Customer Policy," 2013, http://hackingteam.it/index.php/customer-policy (accessed January 23, 2014).

[232] Adrianne Jeffries, "Meet Hacking Team, the company that helps the police hack you" September 13, 2013, *The Verge*, http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers (accessed February 12, 2014); David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," *International Business Times*, March 13, 2013, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507 (accessed February 12, 2014).

[233] David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," *International Business Times*, March 13, 2013, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507 (accessed February 12, 2014).

According to its publicly available "Customer Policy," Hacking Team applies "a number of precautions to limit potential for … abuse" of their products:[234]

- "We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN."[235]
- "We review potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations."
- "We have established an outside panel of technical experts and legal advisors, unique in our industry, that reviews potential sales. This panel reports directly to the board of directors regarding proposed sales."
- "In HT contracts, we require customers to abide by applicable law. We reserve the right in our contracts to suspend support for our software if we find terms of our contracts are violated. If we suspend support for HT technology, the product soon becomes useless."

In public statements, the company has explained that one technique it employs to prevent abuse of its service is an "audit trail," which allows supervising government officials to monitor how employees are using the software and identify "abuse" of the technology by a "rogue employee."[236]

Hacking Team's Customer Policy also states that the firm conducts ongoing employee training on its policies and procedures. During sales negotiations, the company reviews the following "red flags," among other factors in its policies, in deciding whether to conclude a sale:

- "Statements made by the potential customer either to HT or elsewhere that reflect the potential for abuse."

---

[234] Hacking Team, "Customer Policy," 2013, http://hackingteam.it/index.php/customer-policy (accessed January 23, 2014).

[235] Ethiopia is not currently on the blacklists of sanctioned countries for these entities.

[236] David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," *International Business Times*, March 13, 2013, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507 (accessed February 12, 2014).

- "The potential customer's laws, regulations and practices regarding surveillance including due process requirements."
- "Credible government or non-government reports reflecting that a potential customer could use surveillance technologies to facilitate human rights abuses."[237]

Hacking Team also provides a public email address and "encourages anyone with information about apparent misuse or abuse of [their] systems and solutions to promptly report that information."[238]

Hacking Team has been previously criticized for alleged use of its software to target Mamfakinch, a Moroccan citizen journalist group; Ahmed Mansoor, a human rights activist from the United Arab Emirates (UAE); and a US activist who has been critical of the Gülen movement in Turkey, which has been previously documented by Citizen Lab.[239] In response, a spokesperson for the company stated to news media that the company investigated the incidents involving the Moroccan and UAE activists, which included conversations with various unnamed clients.[240] However, the company did not comment in response to media requests about the outcomes of the investigations, nor the actions the company may have taken.[241]

Human Rights Watch wrote to Hacking Team to verify whether this policy was applied to potential sales in Ethiopia, whether the company discovered any "red flags" during its review process, and to request further detail on the firm's contractual end use and lawfulness requirements. Hacking Team responded that the firm does not "confirm or deny the existence of any individual customer or their country location" to maintain the

[237] Hacking Team, "Customer Policy," 2013, http://hackingteam.it/index.php/customer-policy (accessed January 23, 2014).
[238] Ibid.
[239] Morgan Marquis-Boire "Backdoors are Forever: Hacking Team and the Targeting of Dissent?" Citizen Lab, October 10, 2012, https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/ (accessed January 23, 2014); Kim Zetter, "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments," *Wired*, June 4, 2013, http://www.wired.com/threatlevel/2013/06/spy-tool-sold-to-governments/ (accessed January 23, 2014).
[240] David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," *International Business Times*, March 13, 2013, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507.(accessed February 12, 2014).
[241] Pratap Chatterjee, "Turning the Table on the Trackers: Wikileaks Sniffs out Spy Salesmen," *CorpWatch*, September 6th, 2013, http://www.corpwatch.org/article.php?id=15868&printsafe=1 (accessed February 12, 2014).

confidentiality of law enforcement investigations.[242] Hacking Team also stated that, "we expect our clients to behave responsibly and within the law as it applies to them" and that the firm has previously suspended support for their product where it believes it is being misused.[243]

Though Hacking Team's policy states it does not sell to "blacklisted" countries, human rights abuses related to surveillance and the right to privacy can occur in any country, even those who are not on current sanctions or other restrictive measures lists. Ethiopia is not currently on any sanctions lists among the entities listed in Hacking Team's Customer Policy. In addition, though the company's "audit trail" function may address abuse by rogue employees, this feature does not address abuse by supervising authorities, who may be using the tool to illegally surveil targets and violate rights. Finally, national laws that enable surveillance may be inconsistent with a government's international human rights obligations, raising questions as to what law the firm requires customers to abide by in sales contracts.

It is not clear which Ethiopian agencies would control the use of these tools to infiltrate personal computers. Under the anti-terrorism law, the NISS can install equipment to enable surveillance with a court warrant. However, authorities face very few barriers in law and practice in use of surveillance powers, given the lack of privacy safeguards and independent oversight to prevent abuse. Unlike traditional forms of surveillance, the remote nature of these tactics also allows the government to extend these harms far beyond its borders. Given the high cost of this technology, it may only be intended for very precise targets, rather than broad surveillance.[244]

Trade and export of these tools remains virtually unregulated globally, though they have drawn increased scrutiny and calls for greater control by governments. The UK government has confirmed that trade in malware systems like FinSpy requires a license under UK

---

[242] Email from Eric Rabe, Communications Counsel, Hacking Team, to Human Rights Watch, February 19, 2014. See Appendix 2: Correspondence.

[243] Ibid.

[244] For a sense of the costs of equipment, software licenses, support, and services related to FinFisher, see FinFisher, "FinFisher Pricing, Dreamlab" 2011, http://wikileaks.org/spyfiles/docs/DREAMLAB_2011_FinFPric_en.html (accessed February 12, 2014).

regulations.[245] In September 2012, German Foreign Minister Guido Westerwelle called for an EU-wide ban on the export of surveillance software to authoritarian governments, while the European Parliament, led by Marietje Schaake, a Dutch Member of the European Parliament, has endorsed stricter European controls of surveillance systems.[246]

In December 2013, states participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement) added "surveillance and law enforcement/intelligence gathering tools" (also referred to as "intrusion software") to its dual-use technologies control list.[247] The Wassenaar Arrangement is a multilateral export control regime for conventional arms and a range of dual-use goods and technologies.[248] Participating states agree to employ export controls consistent with control lists maintained by the organization, though exact implementation at the national level is decided by each state.[249] Although exact implementation of newly controlled items is still to be determined, the addition of "intrusion software" to the Wassenaar list demonstrates growing consensus among participating states that these tools, "under certain circumstances, may be detrimental to international and regional

[245] Letter from Francesca Debenham, Treasury Solicitor's Department, United Kingdom Government Legal Service, to Bhatt Murphy Solicitors, August 8, 2012; Letter from Francesca Debenham, Treasury Solicitor's Department, United Kingdom Government Legal Service, to Bhatt Murphy Solicitors, September 11, 2012, https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_11_09_dossier_to_hmrc.pdf (accessed February 12, 2014).

[246] Ben Knight, "German spyware business supports dictators," *Deutsche Welle*, September 19, 2012, http://www.dw.de/german-spyware-business-supports-dictators/a-16249165-1 (accessed February 12, 2014); Marietje Schaake, "European Parliament endorses stricter European export control of digital arms," October 23, 2012, http://www.marietjeschaake.eu/2012/10/ep-steunt-d66-initiatief-controle-europese-export-digitale-wapens (accessed February 12, 2014).

[247] Wassenaar Arrangement, "Public Statement, 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies," 2013, http://www.wassenaar.org/publicdocuments/2013/WA%20Plenary%20Public%20Statement%202013.pdf (accessed February 12, 2014); Wassenaar Arrangement, "List of Dual-Use Goods & Technologies and Munitions List," December 2013, http://www.wassenaar.org/controllists/2013/Summary%20of%20Changes%20to%20Control%20Lists%202013.pdf (accessed February 12, 2014); Wassenaar Arrangement, "Control Lists - Current Lists of Dual Use Goods and Technologies and Munitions List," http://www.wassenaar.org/controllists/index.html (accessed February 12, 2014), Category 4.

[248] Wassenaar Arrangement, "Introduction," undated, http://www.wassenaar.org/introduction/index.html (accessed February 12, 2014).

[249] Participating states include Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and United States. Wassenaar Arrangement, "Introduction," undated, http://www.wassenaar.org/introduction/index.html (accessed February 12, 2014).

security and stability."[250] This action may initiate further reforms at the national level to begin controlling the sale of powerful new kinds of surveillance technology.

Other Surveillance Technologies

Ethiopia has also taken steps to acquire additional forms of surveillance technology, including unmanned aerial vehicles (UAVs or drones), which, without appropriate safeguards could be used in violation of basic rights. Surveillance drones were acquired from Israeli company Bluebird Systems in 2011, and Tesfaye Daba, chairperson for the Foreign, Defense and Security Affairs Standing Committee at the Ethiopian Parliament, reported in early 2013 that Ethiopia was now manufacturing its own drones.[251] While former Ethiopian intelligence officers told Human Rights Watch these drones are being used to monitor border areas and are not intended to monitor domestic activities, given the abuse of the surveillance system seen through Ethiopia's telecom sector, there is cause for concern about the use of these technologies.[252]

Jamming of Radio and Television Signals

The Ethiopian government restricts access to information by deliberately jamming radio and television broadcasts of independent and foreign stations. Radio is a key medium for the transmission of independent, reliable, and critical analysis given that the majority of Ethiopians live in rural areas with minimal access to print, television, or Internet media.

Radio jamming has been documented since 2004 when the Eritrean state-run radio Voice of the Broad Masses of Eritrea (VOBME) was frequently jammed. There were also anecdotal reports of the Voice of America (VOA) being jammed at that time. Techniques were primitive but effective, like transmitting white noise from locations in Northern Tigray. This is still the dominant technique used to jam in Ethiopia.[253] In 2007, the TPLF-run Voice of

---

[250] Wassenaar Arrangement, "Public Statement, 2013 Plenary Meeting ."

[251] "Ethiopia buys unmanned aerial vehicles from Bluebird" *defenceWeb*, May 23, 2011, http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=15527:ethiopia-buys-unmanned-aerial-vehicles-from-bluebird&catid=35:Aerospace&Itemid=107 (accessed April 13, 2013) and "MP confirms Ethiopia's Drone Produce," *De Birhan*, February 16, 2013, http://debirhan.com/?p=39 (accessed March 13, 2013).

[252] Human Rights Watch interview with former government official #51, (location withheld), August 2013.

[253] You can hear what "white noise" jamming sounds like during a Radio Xoriyo broadcast at: Radio Xoriyo Somali, 2012, http://sonna.net/content/26102012-radio-xoriyo-somali-1612-17870-sof (accessed February 12, 2014). Radio Xoriyo is a radio station affiliated with the banned ONLF.

the Tigray Revolution was being transmitted from Mekele in northern Ethiopia on the same frequencies as VOBME but at a much higher output, drowning out the VOBME broadcast.[254] In 2009 the government increased its jamming of radio stations that offer independent reporting. Amharic radio broadcasts from VOA and Deutsche Welle (DW) were frequently jammed.[255] DW was jammed regularly after its Amharic language programs criticized the government crackdowns in the aftermath of the 2005 elections. The jamming of DW increased in 2007 and 2008, only reducing slightly after the intervention of senior German government diplomats in 2008. VOA broadcasts in Tigrinya are typically not jammed, but their Afan Oromo broadcasts sometimes are. Local and diaspora radio stations also report being frequently jammed including stations operated by the Ethiopian People's Revolutionary Party (EPRP), Ginbot 7, the OLF, and the ONLF.[256]

Jamming has traditionally increased at politically sensitive times. For instance, during the 2010 parliamentary elections, VOA and DW programs were sometimes unavailable for several days. Programs that are advertised ahead of time covering sensitive political topics (the OLF or ONLF for example) were often being jammed. Jamming typically ceased immediately once less sensitive programs begin broadcasting.[257] A US Embassy cable leaked by WikiLeaks noted that the incidence of VOA jamming increases "in line with GoE (Government of Ethiopia) protests about VOA content."[258]

In August 2012, frequency monitoring revealed that DW programming was blocked on at least one of their three frequencies in Ethiopia 60 percent of the time (18 days out of 30). DW was jammed on all three frequencies 30 percent of the time (on 9 of the 30 days). By contrast, in January 2013 there was no jamming of DW radio transmissions, only for

---

[254] Hans Johnson, "Ethiopia adopts new tactic in radio jamming," post to "Shortwave Central" (blog), December 20, 2007, http://mt-shortwave.blogspot.ca/2007/12/ethiopia-adopts-new-tactic-in-radio.html (accessed March 14, 2013).

[255] The Voice of America is a multi-media international broadcasting service funded by the US government. VOA broadcasts more than 1,500 hours of news and other programming every week in 45 languages to an audience of more than 125 million people. VOA broadcasts to Ethiopia in Amharic, Tigrinya, and Afan Oromo, in addition to English. Deutsche Welle is Germany's international broadcaster and broadcasts in Amharic and English.

[256] The EPRP is Ethiopia's oldest political party. Ginbot 7, the Oromo Liberation Front (OLF), and the Ogaden National Liberation front (ONLF) have all been declared terrorist organizations by the Ethiopian government under the Anti-Terrorism Proclamation.

[257] Human Rights Watch interview with Ludger Schadomsky, editor-in-chief, Deutsche Welle, Bonn, Germany, March 2013 and Human Rights Watch interview with Peter Heinlein, chief, Horn of Africa Service, VOA, Washington, DC, April 2013.

[258] US Department of State, "PM's advisor Bereket Discuss Elections and VOA with PDAs," Wikileaks Canonical ID# 08ADDISABABA214_a, January 29, 2008, https://www.wikileaks.org/plusd/cables/08ADDISABABA214_a.html (accessed February 12, 2014).

jamming to start again in mid-February 2013.[259] DW reports that satellite radio and web-based broadcasts have not been interfered with, and that since March 2013 to date, jamming of their radio transmissions had stopped entirely.[260] VOA also reports a similar lack of jamming in that time.[261] In 2012, DW was accused by diaspora groups of practicing self-censorship and limiting the extent they were willing to criticize government in order to be able to continue working in Ethiopia. DW denied this accusation in an open letter to Ethiomedia.[262] Regardless of the validity of this allegation, ongoing threats to the media leave media with a stark choice: practice restraint and self-censorship in order to operate securely in the country or stop operating. This choice has the most immediate effect on Ethiopian journalists and those working for international media as stringers, but the ability to jam foreign radio broadcasts and block foreign media websites means that foreign media also have to weigh practicing self-censorship against losing access to Ethiopian audiences entirely.[263]

DW has engaged regularly with the government of Ethiopia in an attempt to resolve the jamming situation. Ludger Schadomsky, editor-in-chief of DW Amharic service, told Human Rights Watch:

> In our meetings with the government of Ethiopia we were told by the government representatives "that we jam DW on the grounds of national security. DW is a threat to our national security." Subsequently, they would pull out a huge file with all our show transcripts with lots of red pen—"this was biased, you didn't ask government for an opinion here" and so on and so forth. It is very frustrating, we often set up appointments with different ministers and spokespeople, then when the time comes for the interview their phone is off…. We have brought this up at the highest levels with the

[259] Deutsche Welle jamming monitoring spreadsheets: June 2012- March 2013. Documents on file with Human Rights Watch.

[260] Email communication from Ludger Shadomsky, editor-in-chief, Deutsche Welle to Human Rights Watch, October 2013.

[261] Email communication from Peter Heinlein, chief, Horn of Africa Service, VOA to Human Rights Watch, October 2013.

[262] Ludger Schadomsky, "Open Letter to Ethiomedia.com," *Ethiomedia*, January 11, 2012, http://www.ethiomedia.com/broad/3402.html (accessed March 13, 2014).

[263] The government has used various additional means to make it difficult for VOA and other international organizations to operate in Ethiopia including the regular detention of journalists and denial of work permits.

> German government and the German ambassador. The German ambassador has had discussions with Bereket and nothing has changed.[264]

In contrast to its handling of DW, the Ethiopian government has chosen not to engage in any substantive conversation with VOA officials about these issues.[265] Meles Zenawi famously stated in 2010 in response to a question from a VOA reporter about jamming that, "we have for some time now been trying to beef up our capacity to deal with this, including … jamming." He also compared the VOA broadcasts to the Rwandan radio station Mille Collines, which was implicated in inciting genocide in 1994, calling VOA broadcasts "destabilizing propaganda."[266] The US government publicly criticized the jamming of VOA in March 2010 stating that the "decision to jam VOA broadcasts contradicts the Government of Ethiopia's frequent public commitments to freedom of the press."[267]

Broadcasters have used different techniques to get around jamming including changing frequencies, moving to satellite radio, transmitting on different bands (FW vs. medium wave vs. shortwave), and increasing their web presence. All of these options are expensive and out of reach to all but the largest international media outlets.

While the jamming of radio stations is relatively inexpensive and technically simple, the jamming of television stations is much more expensive and energy-intensive. There are no independent television stations based in Ethiopia. However since 2010, Ethiopian Satellite Television (ESAT), a popular diaspora-run satellite television station, reports being frequently jammed. Ethiopian government often accuses ESAT of being a mouthpiece for Ginbot 7. The government of Ethiopia convicted three ESAT employees under the anti-terrorism law in July 2012. They were tried *in absentia* and sentenced to 15 years each. All

---

[264] Human Rights Watch Interview with Ludger Schadomsky, editor-in-chief, Deutsche Welle Amharic, Bonn, Germany, March 2013 and Human Rights Watch interview with Peter Heinlein, chief, Horn of Africa Service, VOA, Washington, DC, April 2013.

[265] "US Criticized Ethiopia for Jamming VOA Signals," *Voice of America*, March 19, 2010, http://www.voanews.com/content/ethiopia-criticized-by-us-for-jamming-voa-signals-88733542/153788.html (accessed March 14, 2014)

[266] "Ethiopia admits jamming VOA radio broadcasts in Amharic," *BBC*, March 19, 2010, http://news.bbc.co.uk/2/hi/8575749.stm (accessed March 4 2013).

[267] US Department of State, "United States Strongly Criticizes Ethiopia's Jamming of Voice of America," March 19, 2013, http://www.state.gov/r/pa/prs/ps/2010/03/138682.htm (accessed February 12, 2014).

three live in the US. The Ethiopian government also regularly jams EritTV, the Eritrean state-run television station.[268]

Ethiopia has reportedly used both orbital jamming and terrestrial jamming[269] to jam satellite television transmissions.[270] One individual who was working with Egyptian-owned Nilesat on an unrelated technical issue told Human Rights Watch that individuals from INSA came and visited him in late 2010 to find the upload frequencies for Nilesat because they wanted to "jam one foreign station."[271] When the government chooses to jam a station on a satellite provider such as Nilesat, this has the unintended outcome of jamming many of the other stations that also use that satellite. For example, in early 2012, reports suggested that jamming originating from Ethiopia was responsible for blocked stations on Saudi-based Arabsat as far away as Lebanon. This prompted a complaint from Lebanese authorities.[272]

These practices put these satellite providers in a difficult predicament: if they agree to host a channel that could be jammed, this endangers all its other programming. In response to this, a variety of satellite providers have required increased security deposits or other guarantees should they host ESAT. Several satellite providers have told ESAT that the Ethiopian government has contacted them to pressure them not to host ESAT.[273] Use of jamming and exerting of pressure from government of Ethiopia has

---

[268] "PM's advisor Bereket Discuss Elections and VOA with PDAs," Wikileaks, January 29, 2008, https://www.wikileaks.org/plusd/cables/08ADDISABABA214_a.html (accessed march 14, 2014).

[269] Orbital jamming involves the perpetrator beaming contradictory signals directly towards a satellite via a rogue uplink station. When these jamming signals are sent, frequencies become mixed with each other and the targeted channel's feed is completely overridden for everyone, everywhere. In addition, as satellite capacity operates in groups of channels, when one channel is jammed, all others in the same group are also affected. Terrestrial jamming takes place in a specific location and involves equipment that is easy to purchase, use and conceal. Rather than targeting the satellite itself, as is the case in orbital jamming, terrestrial jamming involves transmitting rogue frequencies in the direction of local consumer-level satellite dishes. The contradictory frequencies are area-specific, interfering only with the frequency emanating from the satellite in a specific location. Small, portable terrestrial jammers have a range of 3-5 kilometers in urban, built-up areas. In rural areas, their range can increase to up to 20 kilometers. From "Satellite Jamming in Iran: A war over Airwaves," A Small Media Report, November 2012, http://www-tc.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf (accessed July 13, 2013).

[270] Human Rights Watch interview #47 (name and location withheld), May 2013.

[271] Human Rights Watch interview #25 (name and location withheld), April 2013.

[272] "Jamming of Arabsat coming from Ethiopia," *Daily Star*, February 16, 2012, http://www.dailystar.com.lb/News/Local-News/2012/Feb-16/163438-sehnaoui-jamming-of-arabsat-coming-from-ethiopia.ashx#ixzz1mVTDna2w (accessed September 4, 2013).

[273] Human Rights Watch interview with ESAT employees, Washington, DC, December 2012.

resulted in ESAT being jammed or removed from Arabsat, Nilesat, Thaicon, and Intelset.[274] ESAT reports being jammed at least 10 different times in Ethiopia since its April 2010 launch, but its television service has not been jammed regularly in Ethiopia since October 2012.[275]

ESAT's shortwave radio broadcasts are also routinely jammed. Human Rights Watch and Citizen Lab testing found that ESAT's website was blocked and unavailable in Ethiopia as of August 2013.[276] As the Ethiopian economy grows and the middle class increases in size, more and more Ethiopians are turning to ESAT and other foreign television stations for access to independent information on Ethiopian affairs.

It is not clear which technologies are used to jam radio and television, but standard jamming technologies are generally affordable and easy to obtain.[277] Jamming techniques employed in Ethiopia are rudimentary but quite energy intensive. Numerous former government officials told Human Rights Watch that new jamming technologies are being tested that would result in complete jamming of targeted programs, use less energy, and be more precise.[278] These claims could not be verified. Former Ethio Telecom officials told Human Rights Watch that the transmission of jamming signals occurs from Ethio Telecom operated facilities from both inside and outside of Addis.[279]

Beyond its effects on the free expression rights of Ethiopians, the deliberate jamming of commercial radio and television broadcasts contravenes ITU regulations.[280]

---

[274] Ethiopian Freepress Journalists' Association, "EFJA urges China to stop complicity in jamming satellite TV transmissions," June 22, 2011, http://reliefweb.int/report/china/efja-urges-china-stop-complicity-jamming-ethiopian-satellite-tv-transmissions (accessed January 11, 2013).

[275] ESAT, "ESAT resumes broadcast on Amos Satellite," December 20, 2012, http://ethsat.com/2012/12/20/esat-resumes-broadcast-on-amos-satellite/ (accessed January 8, 2013) and Human Rights Watch interview with ESAT employee #103, (location withheld,) November 2013.

[276] Human Rights Watch/Citizen Lab Internet filtering testing, July 2013 and August 2013.

[277] "Satellite Jamming in Iran: A war over Airwaves," A Small Media Report, November 2012, http://www-tc.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf) (accessed July 13, 2013).

[278] Human Rights Watch interviews with former government officials#49 and 51, (locations withheld), May 2013.

[279] Human Rights Watch interview with former government employee #14, (location withheld), February 2013.

[280] ITU Constitution, article 15; ITU Radio Regulations, article 15. Ethiopia joined the ITU in 1932.

III. Legal Context

International Law

Ethiopia is a party to major international and regional human rights conventions, including the International Covenant on Civil and Political Rights (ICCPR)[281] and the African Charter on Human and Peoples' Rights (the African Charter).[282] These multinational treaties set out fundamental rights including rights to the security of the person; to liberty of movement; to be free from arbitrary arrest and detention; to privacy; and to freedom of opinion, expression, and association.

In 2011, the United Nations' preeminent human rights body, the Human Rights Council, affirmed that "the same rights that people have offline must also be protected online."[283] While these rights are not absolute, any limitations of these rights must meet specific criteria under international law.

Freedom of Expression

Article 19 of the ICCPR guarantees the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers," in any medium, including through Internet or mobile networks.[284] The ICCPR provides that any limitation on the right to freedom of expression must be provided by law that is clear and accessible to the public; must be designed to protect public order, national security, or other legitimate purposes; and must be necessary, proportionate, and use the least restrictive means to achieve the legitimate aim.[285]

---

[281] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976. Ethiopia ratified the ICCPR in 1993.

[282] African [Banjul] Charter on Human and Peoples' Rights (the African Charter), adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986. Ethiopia ratified the African Charter in 1998.

[283] UN Human Rights Council (UN HRC), "The promotion, protection and enjoyment of human rights on the Internet," Resolution 20 (2012), U.N. Doc A/HRC/20/L.13, http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf (accessed October 11, 2013).

[284] Report of the special rapporteur on the Internet, para. 20 ("the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression.)

[285] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, September 12, 2011, U.N. Doc. CCPR/C/GC/34, http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf (accessed February 12, 2014).

Article 9 of the African Charter guarantees that every individual shall have the "right to receive information" and "to express and disseminate his opinions within the law."[286] The charter also provides for the right to freedom of association and assembly with others.[287]

The special rapporteur on the right to freedom of expression has specifically addressed the permissibility of Internet filtering under international law, expressing that he was:

> [D]eeply concerned by increasingly sophisticated blocking or filtering mechanisms used by States for censorship. The lack of transparency surrounding these measures also makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by States.[288]

The special rapporteur called upon governments that currently block websites to:

> [P]rovide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on the affected websites as to why they have been blocked. Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences.[289]

The special rapporteur has also stated that measures to cut off access to the Internet or mobile service entirely, regardless of the justification provided, are "disproportionate and thus a violation of article 19."[290] The rapporteur has called on all states to ensure network access is maintained at all times, including during times of political unrest.[291] The special

---

OHCHR, "Freedom of Opinion and Expression - Annual reports," 2013, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx (accessed February 12, 2014).

[286] African Charter, art. 9.

[287] African Charter, arts. 10-11.

[288] Report of the special rapporteur on the Internet , para. 70.

[289] Ibid.

[290] Report of the special rapporteur on the Internet, para. 78.

[291] Ibid.

rapporteur on freedom of expression and access to information in Africa has also affirmed many of these principles in a 2011 joint declaration.[292]

Right to Privacy

Article 17 of the ICCPR provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and "[e]veryone has the right to the protection of the law against such interference or attacks." The special rapporteur on freedom of expression has interpreted "correspondence" to encompass all forms of communication, both online and offline.[293]

Limitations on the right to privacy similarly must be prescribed by law, necessary to achieve a legitimate aim, and proportional and narrowly tailored to achieving the aim.[294] The special rapporteur on freedom of expression has stated that:

> Communications surveillance should be regarded as a highly intrusive act.... Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope, and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[295]

To be prescribed by law, limitations on the right to privacy must meet "a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their applications."[296] The principle of proportionality requires

---

[292] OSCE, "International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet," June 1, 2011, http://www.osce.org/fom/78309 (accessed March 14, 2014).

[293] Report of the special rapporteur on surveillance, para. 24.

[294] See Report of the special rapporteur on surveillance. UN HRC, Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, ("Report of the special rapporteur on human rights and counterterrorism,") December 28, 2009, U.N. Doc. A/HRC/13/37, paras. 17-18.

[295] Report of the special rapporteur on surveillance, para. 81.

[296] Report of the special rapporteur on surveillance, para. 83.

that any surveillance measure must not be employed when less invasive techniques are available, and must be proportionate to the interest to be protected.[297]

As the special rapporteur on human rights and counterterrorism explains, these principles apply even where the stated aim of surveillance is countering terrorism: "there must be no secret surveillance that is not under the review of an effective oversight body and all interferences must be authorized through an independent body."[298]

Finally, the special rapporteur on freedom of expression has addressed the legality of real-name registration policies and offensive intrusion tactics (that is, secretly infiltrating a computer to steal files or monitor activity). The special rapporteur has called on governments to ensure individuals can "express themselves anonymously online and to refrain from adopting real-name registration systems."[299] Governments should "refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés, or mobile telephony."[300] In addition, offensive intrusion tactics—methods that involve hacking into computers or networks—threaten "the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings."[301]

Responsibilities of Companies

Companies have a responsibility to respect human rights. This principle is reflected in the United Nations "Protect, Respect, and Remedy" Framework[302] and the UN Guiding Principles on Business and Human Rights,[303] which are widely accepted by

---

[297] Report of the special rapporteur on surveillance, para. 83.

[298] Report of the special rapporteur on human rights counterterrorism, para. 62.

[299] Report of the special rapporteur on the Internet, para. 84.

[300] Report of the special rapporteur on surveillance, para 88.

[301] Report of the special rapporteur on surveillance, paras. 62-63. Offensive intrusion tactics often involve hacking into computers and systems and copying, deleting, or altering electronic information or computer code.

[302] UN HRC, "Protect, Respect and Remedy: a Framework for Business and Human Rights," U.N. Doc. A/HRC/8/5, April 7 2008, http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf (accessed April 10, 2013).

[303] UN OHCHR, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect, and Remedy' Framework," U.N. Doc. HR/PUB/11/04, 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (accessed April 10, 2013).

companies and governments. This principle is also incorporated into industry-specific human rights initiatives such as the Global Network Initiative, a global multi-stakeholder initiative that aims to ensure technology companies respect the rights to freedom of expression and privacy online.[304]

The corporate responsibility to respect contemplates that companies should undertake credible human rights due diligence and mitigate human rights risks so that their operations do not facilitate or exacerbate human rights problems. Specifically, the Global Network Initiative Principles and Guidelines and UN Guiding Principles call on companies to:

- Conduct rigorous due diligence and put in place procedures to identify, prevent, mitigate, and account for how they address their impacts on human rights.
- Employ human rights impact assessments to identify circumstances when freedom of expression and privacy may be jeopardized or advanced, and develop appropriate risk mitigation strategies. Such assessments should occur in relation to designing and introducing new technologies, entering a new market, taking on business partners, or committing to business contracts or license agreements.
- Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights standards on freedom of expression and privacy. With respect to sales of technology or services, this principle contemplates an inquiry as to the end use and end user of the technology or service, and procedures to prevent misuse of a company's technology or services to facilitate human rights abuses.
- Aggressively challenge or push back when asked to assist with government censorship or illegal surveillance practices inconsistent with international human rights obligations.
- Engage government officials to promote rule of law and the reform of practices that infringe on the rights to freedom of expression and privacy.
-

[304] Global Network Initiative, "Core Commitments," undated, http://www.globalnetworkinitiative.org/corecommitments/index.php (accessed April 10, 2013).

- Put in place processes to enable remediation of any adverse human rights impacts they cause or to which they contribute.

These standards are relevant to companies who may be asked to assist with censorship or illegal surveillance, or who sell technology and services to countries where there is a serious risk that they will be used to violate rights.

These standards were published in 2008. While many of the telecommunications equipment contracts at issue in this report were signed or completed prior to 2008, telecommunications equipment companies should have been adopting and implementing these principles in their operations since 2008, and should address and mitigate any adverse impacts flowing from engagements that began prior to 2008.

Ethiopian Law

The Ethiopian constitution of 1995 formally guarantees the rights to freedom of expression, freedom of the press, access to information, and to privacy.[305] However, in practice, the Ethiopian government maintains strict control over print, broadcast, and online media, as well as access to Internet and mobile services.

Freedom of Expression and Access to Information

Article 29 of the constitution expressly guarantees that everyone has the "right to freedom of expression without any interference ... through any media of his or her choice."[306] It also provides legal protections for freedom of the press and other mass media, guaranteeing access to "information of public interest." Finally, the constitution expressly prohibits "any form of censorship." A number of laws govern freedom of expression, freedom of the media, and access to information.

The Mass Media and Freedom of Information Proclamation of 2008, also known as the press law, appears to reaffirm constitutional protections for mass media, access to publicly held information, and prohibitions on censorship. However, the law in practice

[305] Constitution of the Federal Democratic Republic of Ethiopia, (1995), arts. 26 and 29.
[306] Constitution of the Federal Democratic Republic of Ethiopia, (1995), art. 29.

grants broad government power to initiate defamation suits (regardless of the defamed official's interest), imposes crippling financial penalties, and preserves power to arbitrarily deny licenses and registration.[307] Although the press law makes some positive changes such as barring the pre-trial detention of journalists, since 2008 the threat and application of the use of this and other laws has had the effect of decimating what independent media existed in Ethiopia.[308] It is unclear whether the broad terms of the press law also apply to online media, bloggers, or print or broadcast media that also publish online.

The Telecom Fraud Offence Proclamation addresses use of Internet and mobile technologies specifically.[309] Enacted in 2012, the telecom fraud law criminalizes a range of services and activities related to telecommunications services, defined broadly to include mobile telephone, satellite telephone, and Internet services, while also entrenching the monopoly of the government-owned telecommunications operator. The stated goal of the new law is to address telecom fraud, which purportedly prevents the telecom industry from playing "an essential role in … peace, democratization, and development" and poses "a serious threat to the national security beyond economic losses."[310]

In part, the telecom fraud law restates existing offenses from the Telecom Proclamation of 1996 (as amended in 2002) and increases sanctions for their violation.[311] However, the law also extends the anti-terrorism proclamation and criminal code to online activity. For instance, using a telecom network to disseminate a "terrorizing" or obscene message, or for any other undefined "illegal purpose," is punishable with up to eight years' imprisonment and a fine.[312]

---

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

[308] For an overview of media issues in Ethiopia see: Committee to Protect Journalists, "Ethiopia," 2014, http://www.cpj.org/africa/ethiopia/(accessed February 12, 2014); Article 19, "The Legal Framework for Freedom of Expression in Ethiopia," http://www.article19.org/data/files/pdfs/publications/ethiopia-legal-framework-for-foe.pdf (accessed February 12, 2014); "Ethiopia: Terrorism Law Decimates Media," Human Rights Watch news release, May 3, 2013, http://www.hrw.org/news/2013/05/03/ethiopia-terrorism-law-decimates-media.

[309] Telecom Fraud Offence Proclamation No. 761/2012.

[310] Telecom Fraud Offence Proclamation, Preamble.

[311] Telecommunications Proclamation No. 49/1996, November 28, 1996. http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf (accessed February 12, 2014); Telecommunications (Amendment) Proclamation No. 281/2002, July 2, 2002, http://www.eta.gov.et/Scan/Telecom%20Proc%20281_2002%20(amendment)%20NG.pdf (accessed February 12, 2014).

[312] Telecom Fraud Offence Proclamation, Art. 6.

The phrase "terrorizing message" is not defined in the law, but the provision allows punishment of any electronic message "connected with" a crime punishable under the anti-terrorism law. The deeply flawed Anti-Terrorism Proclamation contains an overly broad definition of terrorism that can encompass even peaceful expressions of dissent and political protest that pose no threat to national security. The law is particularly worrying for online and offline media because it provides discretion to authorities to prosecute those who "promote" or encourage terrorism. Under the law's broad definition, this could include bloggers, editors, and journalists who publish articles referring to armed opposition movements, such as the Oromo Liberation Front or the Ogaden National Liberation Front, or any other individuals or groups deemed as terrorists, "anti-people," or "anti-peace" by the government.

The telecom fraud law also criminalizes commercial provision and use of voice over Internet protocol (VoIP) services like Skype or Google Talk, or services that otherwise "bypass" Ethio Telecom infrastructure.[313] Several government officials have issued statements at the time of the law's enactment affirming Skype's legality, especially for personal use.[314]

As discussed in further detail in the Controlling the Internet section of this report, the state-controlled telecom operator Ethio Telecom engages in filtering and blocking of websites. However, the legal basis for this practice is unclear.

Right to Privacy

The Ethiopian constitution specifically guarantees the "inviolability of "notes and correspondence," including "communications made by means of telephone, telecommunications and electronic devices."[315] The constitution also provides that "public officials shall respect and protect these rights," and "no restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws" and specific purposes. The telecom fraud law punishes interception and

[313] Telecom Fraud Offence Proclamation, Arts. 9, 10(3)-(4). This prohibition has been in place since the Telecommunications Proclamation was amended in 2002. See Telecommunications (Amendment) Proclamation, art. 2(11). However, the new telecom fraud law increases the penalties available.

[314] See, for example, Ministry of Foreign Affairs, "Ethiopian Telecom law affirms Skype's legality," July 13, 2012, http://www.mfa.gov.et/news/more.php?newsid=862 (accessed March 14, 2014).

[315] Ethiopian Constitution, art. 26.

illegal access to telecom systems without authorization, and the criminal code punishes a range of computer crimes, including hacking and unauthorized alteration of data.[316]

Surveillance of Internet and phone communications is allowed under several broadly drawn laws, with vague and superficial safeguards for the right to privacy. As a general rule, to issue a search warrant, the Criminal Procedure Code requires that a court must determine that the "purposes of justice or of any inquiry, trial, or other proceedings under this Code will be served," a vague and broadly drawn standard that leaves much discretion to courts.[317]

Under the Anti-Terrorism Proclamation, upon obtaining a court warrant, the National Intelligence and Security Service (NISS) can conduct communications surveillance "to prevent and control a terrorist act," as well as install or remove equipment to enable such surveillance.[318] The anti-terrorism law lists factors for the court to consider in granting a covert search warrant, including the extent to which measures would assist in preventing terrorism. However, the law does not impose any specific standards or rules to limit court discretion in granting a search warrant. In addition, there is no requirement to disclose any information about how evidence from intelligence reports presented in terrorism cases was gathered, which prevents the ability to challenge use of evidence gathered through illegal surveillance.[319]

Communications service providers are required to cooperate with requests from NISS for assistance.[320] The anti-terrorism law also imposes a duty on individuals and private organizations to produce information or evidence that the police "reasonably believes could assist to prevent or investigate terrorism cases."[321]

These provisions are overly broad, and prone to misuse by a government that uses its legislation to target opposition politicians, journalists, and others who oppose government policies.

---

[316] Telecom Fraud Offence Proclamation, art. 5; Criminal Code, arts. 706-711.

[317] Criminal Procedure Code of Ethiopia, Proclamation No. 185/1961, art. 33.

[318] Anti-Terrorism Proclamation, art. 14.

[319] Anti-Terrorism Proclamation, art. 23.

[320] NISS Proclamation, art. 27.

[321] Anti-Terrorism Proclamation, art. 22. Breach of this duty is punishable with up to 10 years of rigorous imprisonment. Anti-Terrorism Proclamation art. 35.

Under a newly-enacted law re-establishing the NISS, this ministerial-level agency has broad powers to conduct surveillance on any person suspected of a range of criminal activities in order to protect national security.[322] These powers are nominally subject to legislative and executive oversight, but the contours of such oversight are undefined. Surveillance requires a court warrant, but the law imposes no procedures or limitations on when courts may grant a search warrant.[323] Given the breadth of the agency's mandate and the lack of specific safeguards that limit the nature, scope, and duration of the NISS's surveillance powers, the law leaves undue discretion to the agency and raises concerns about abuse of these powers to target those who might criticize or oppose government policies.

Surveillance conducted under the money laundering and terrorist financing law is subject to a slightly more defined standard: courts can authorize "access to computer systems, networks, and servers" and surveillance of communications if there are "serious indications" that such computer systems and networks or telephone lines are or may be used by persons suspected of money laundering or financing of terrorism.[324] In practice, the law is broad enough to encompass the activities of nongovernmental organizations and other civil society groups, who could then become targets of such surveillance. [325]

Finally, under the telecom fraud law, police may apply for a covert search warrant from the Federal High Court where they have "reasonable ground" to believe that telecom fraud is "likely" to be committed, which allows collection of electronic evidence and evidence gathered through surveillance.[326]

In all, the broad surveillance powers articulated in these laws do not meet a level of clarity and precision required for such limitations to be prescribed by law. The lack of legal safeguards that limit the nature, scope, and duration of surveillance measures, and grounds

---

[322] National Intelligence and Security Service Re-establishment Proclamation, No. 804/2013,

[323] National Intelligence and Security Service Re-establishment Proclamation, arts. 8, 22-24.

[324] Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013, February 4, 2013, Federal Negarit Gazette, arts. 25 and 52. In addition, the anti-corruption law allows the head of the "appropriate organ" to approve searches and interceptions of electronic communications where "necessary for the investigation of corruption offence." Revised Proclamation to Provide For Special Procedure and Rules of Evidence on Anti-Corruption, Proclamation No. 434/2005, February 2, 2005, Federal Negarit Gazeta, art. 46.

[325] Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation 657/2009, s12.

[326] Telecom Fraud Offence Proclamation, arts. 14-16.

for judicial approval, raises concerns that these powers are not adequately regulated to prevent arbitrary, unlawful, or disproportionate interference with the right to privacy.

Although court warrants are required for some forms of surveillance, the courts seem to play no ongoing oversight role to safeguard against abuses in carrying out the warrant or over how personal information collected through surveillance is used. Although Ethiopian law provides for an independent judiciary, criminal courts remain subject to political influence, raising concerns that even weak safeguards may be further undermined, especially in cases involving politically sensitive issues of national security.[327] In any case, there appears to be almost no ability to challenge the legality of surveillance and no rule to exclude illegally obtained evidence in criminal proceedings. In practice, it seems much surveillance may be conducted without a warrant.

Lastly, individuals are asked to register with their real name in order to purchase a mobile SIM card or access the Internet at Internet cafés. For Internet cafes, reports emerged in 2006 that the ETA ordered café owners to register and maintain a log of Internet users, and the government has closed cafés in the past for various violations, in particular use of VoIP services.[328] In practice, today this requirement is not consistently enforced. However, in contrast, the requirement for SIM card registration is far more rigidly enforced.

The legal basis for both these practices is unclear and available laws and regulations do not address the requirement. The 2012 telecom fraud law punishes obtaining a telecom service through "fraudulent means," including by "using the identity code of another person."[329] Because the state retains a monopoly mobile telephony and cybercafés must be licensed by the MCIT, real-name registration requirements might be addressed in individual license agreements, but Human Rights Watch has been unable to confirm.[330] Such practices do not appear to be regulated in law.

---

[327] See Human Rights Watch, *"They Want a Confession."*

[328] See Groum Abate, "Ethiopia Internet cafes start registering users," *Capital*, December 27, 2006, http://nazret.com/blog/index.php/2006/12/27/ethiopia_internet_cafes_start_registerin (accessed March 14, 2014).

[329] Telecom Fraud Offence Proclamation, art. 10(2).

[330] The 2002 Resale and Telecenter Directives does not include real name registration obligations for licensed Internet resellers (e.g., Internet cafés). Ethiopian Telecommunication Agency, "License Directive for Resale and Telecenter in Telecommunication Service," November 8, 2002, http://www.eta.gov.et/Word/DRAFTRESALEDIRECTIVE(ENG).pdf (accessed March 14, 2014).

IV. The Future of Ethiopia's Telecommunications Surveillance Capacity

The spread of information that would normally be taken as a given in many countries is limited in Ethiopia through a combination of repressive laws, lack of independence of media, jamming of radio and television stations and blocking of websites—all of which adds to existing fears of government oppression. In absence of a free and vibrant media, mobile and Internet communication can play an important role in the spread of ideas and perspectives. Telecom surveillance and, equally as important, the perception of pervasive telecom surveillance serves to limit the usefulness of these technologies to the ultimate betterment of society.

There is little doubt that surveillance is pervasive at every level of life in Ethiopia. But the use of advanced telecom surveillance technologies is still in its infancy. As this report shows, mobile telephone surveillance happens regularly and the technical potential exists for nearly *any* communication to be monitored in Ethiopia. Presently, this monitoring takes a considerable amount of human capacity, which severely restricts Ethiopia's ability to monitor telecommunications on a large scale. While there is limited evidence available on specific cases where emails were intercepted or other Internet-based communication was monitored, the Ethiopian government has acquired the best technologies to do so. The government's capacity to further restrict privacy rights, access to information, and freedoms of expression, association, and peaceful assembly will grow as their ability to use the acquired advanced technologies grows—unless serious efforts are made, particularly by international donors, concerned governments, and the telecommunications industry, to reverse this disturbing trajectory.

Acknowledgments

This report was researched and written by Felix Horne, researcher in the Africa division and Cynthia Wong, senior Internet researcher at Human Rights Watch. It was edited by Leslie Lefkow, deputy director of the Africa division and Arvind Ganesan, director of the business and human rights division. James Ross, legal and policy director, and Babatunde Olugboji, deputy program director, provided legal and program review. Jessica Evans, senior researcher/advocate for International Financial Institutions reviewed the section on international donors, and Nicholas Bequelin, senior researcher in the Asia division reviewed sections on Chinese firms.

Report production and editorial assistance was provided by Darcy Milburn, senior associate in the business and human rights division; Grace Choi, publications director; Kathy Mills, publications specialist; and Fitzroy Hepkins, administrative manager.

Internet filtering and malware testing was carried out in partnership with researchers at the University of Toronto's Citizen Lab.

Human Rights Watch would like to thank partners at Citizen Lab, especially Bill Marczak, Electronic Frontier Foundation, and Privacy International for their assistance and support. We also thank all of the individuals who shared their experiences, despite concern of reprisals, for making this report possible.

Appendix 1: A Sampling of Blocked Websites in Ethiopia

Because Internet filtering is not transparent in Ethiopia, it can be difficult to separate transient network issues that may make a website inaccessible from deliberate interference by the telecom operator or another third party. However, the testing methodology developed by Citizen Lab prioritizes the minimization of false positives. This list is not comprehensive and only provides a sampling of the websites found to be blocked in 2013 testing. The absence of a website from the list of blocked URLs does not necessarily mean the site is accessible in Ethiopia. In addition, because the list of websites tested is not comprehensive, results may underestimate the extent of material that is blocked.

Category	URL	Website	Content
Blog	http://yekolotemari.blog.com	Aqumada	Personal blog
Blog	http://www.ethiopundit.blogspot.com	Ethiopundit	Ethiopia-related blog
Blog	http://www.seminawork.blogspot.com	Ethio-Zagol Post: The State of Ethiopia	Ethiopia-related political blog
Blog	http://www.mediaethiopia.com/blog/	MediaEthiopia.com	Ethiopia-related political blog
Blog	http://www.mesfinwoldemariam.org	Mesfin Woldemariam	Site is Under Construction
Blog	http://www.meskelsquare.com	Meskel square	Ethiopia-related blog by a London-based journalist
Blog	http://tegbar.org/	Tegbar	Ethiopia-related blog
Chat room	http://www.cyberethiopia.com/warka4/	Cyber Ethiopia, Hanina	Chat rooms for CyberEthiopia
Media	http://www.addisnegeronline.com	Addis Neger	Official website of the Ethiopian Addis Neger newspaper
Media	http://www.addisvoice.com	Addis Voice	Ethiopian media aggregator website

Category	URL	Website	Content
Media	http://www.cyberethiopia.com	CyberEthiopia	CyberEthiopia.com is registered as a non-profit association in Geneva, Switzerland
Media	http://www.debteraw.com	Debteraw: Ethiopian News and Politics Journal	Ethiopia-related political website started by Ethiopians residing in London
Media	http://www.ethiomedia.com/index.html	Ethiomedia.com	Ethiopia related media site
Media	http://ethiox.com	Ethiopia Exchange	Ethiopia and Horn of Africa related news, articles, and opinions
Media	http://www.ethioforum.org	Ethiopian Media Forum	Ethiopia and Horn of Africa related news analysis created by exiled journalists
Media	http://ethiopianreview.com	Ethiopian Review	Ethiopian media website
Media	http://ethsat.com/	Ethiopian Satellite Television	Ethiopia-related media site
Media	http://www.gambelatoday.com/	Gambela Today	Website for news organization based in the US
Media	http://www.goolgule.com/	Golgul	Mainly Amharic language Ethiopia-related media site
Media	http://www.ethiopians.com/hright.html	Human Rights Files Pertaining to Ethiopia	Reports on human rights abuses in Ethiopia
Media	http://www.ethiopians.com	MediaEthiopia.com	Ethiopia related news, articles, and opinions
Media	http://www.mediaethiopia.com	MediaEthiopia.com	Ethiopia-related media site
Media	http://nazret.com	Nazret.com	Ethiopian media

Category	URL	Website	Content
			site
Media	http://nazret.com/blog/index.php?blog=9	Nazret.com, AddisFerengi	French section of the Ethiopian Media site
Media	http://nazret.com/blog/index.php?blog=14	Nazret.com, Afan Oromo	Afan Oromo language section of the Ethiopian media site
Media	http://nazret.com/blog/index.php?blog=12	Nazret.com, Commentary	Commentary - useful tips for co-existence and prosperity section of the Ethiopian media site
Media	http://nazret.com/blog/index.php?blog=16	Nazret.com, Community Bulletin	Community Bulletin section of the Ethiopian media site
Media	http://nazret.com/blog/index.php?blog=15	Nazret.com, Merkato	Merkato Blog - marketplace for ideas section of the Ethiopian media site
Media	http://nazret.com/blog/index.php?blog=7	Nazret.com, Sport	Sports section of the Ethiopian Media site
Media	http://nazret.com/blog/index.php?blog=13	Nazret.com, Urael	Business section of the Ethiopian media site
Media	http://www.ogaden.com	Ogaden Online	Media site for Ogaden in particular and the Horn of Africa region
Media	http://www.oromia.org	Oromia Online	Ethiopia and Oromia specific media website
Media	http://www.quatero.net	Quatero News and Views	Ethiopian media website
Media	http://www.tigrai.org	Tigray.net	Tigray media website

Category	URL	Website	Content
Media	http://www.tzta.ca	TZTA	Ethiopia-related news site based in Canada
Nongovernmental organization	http://www.anuakjustice.org	Anuak Justice Council	Non-profit organization representing the Anuak people of Gambella, Ethiopia
Nongovernmental organization	http://www.socepp.de	Solidarity Committee for Ethiopian Political Prisoners	Information on the human rights situation in Ethiopia
Nongovernmental organization	http://solidaritymovement.org/	Solidarity Movement for a New Ethiopia	Website for social justice movement in Ethiopia
Armed opposition movement	http://www.eppf.net	Ethiopian People's Patriotic Front	Official website of the Ethiopian People's Patriotic Front
Banned opposition movement	http://www.ginbot7.com	Official Site for Ginbot 7 Movement for Justice, Freedom, and Democracy	Official website for political opposition movement
Banned armed opposition movement	http://www.onlf.org	Ogaden National Liberation Front Website	Website for ONLF social and political movement
Banned armed opposition movement	http://www.oromoliberationfront.org	Oromo Liberation Front	Website for OLF political movement and information on Oromia
Unregistered opposition party	http://www.eprp.com	Ethiopian People's Revolutionary Party (EPRP)	Official website of the Ethiopian People's Revolutionary Party
Unregistered opposition party	http://www.medhin.org	Medhin	The Ethiopian Medhin Democratic Party official website

Appendix 2: Correspondence

Correspondence with the Ethiopian Government

- Human Rights Watch Letter to Dr. Shiferaw Teklemariam, Minister of Federal Affairs, Ministry of Federal Affairs, Government of Ethiopia, February 11, 2014
- Human Rights Watch also sent similar letters to:
    - Dr. Debretsion G. Michael, Minister of Communications and Information Technology, Ministry of Communications and Information Technology, February 11, 2014
    - Dr. Getachew Ambaye, Minister of Justice, Ministry of Justice, February 11, 2014

Correspondence with Businesses

Orange:

- Human Rights Watch Letter to Mr. Stéphane Richard, Chairman and Chief Executive Officer, Orange, October 28, 2013
- Letter from Brigitte Dumont, Chief Officer, Group CSR, Orange, November 19, 2014
- Letter from Human Rights Watch to Mr. Yves Nissim, VP, Head of Transformation and Operation in CSR, and Ms. Brigitte Dumont, Chief Officer, Group CSR, Orange, December 12, 2013
- Letter from Mr. Yves Nissim, VP, Head of Transformation and Operation in CSR, Orange, to Human Rights Watch, January 14, 2014

Huawei:

- Human Rights Watch Letter to Mr. Eric Xu, Acting CEO, Huawei, October 29, 2013
- Letter from Mr. William Plummer, Vice President, External Affairs, Huawei, November 12, 2013

Sinovatio:

- Human Rights Watch Letter to Sinovatio, October 29, 2013

ZTE:

- Human Rights Watch Letter to Mr. Shi Lirong, President and Executive Director, ZTE Corporation, October 29, 2013

Hacking Team:

- Human Rights Watch Letter to Mr. David Vincenzetti, President of the Board, Chief Executive, and Mr. Valeriano Bedeschi, Managing Director, Hacking Team, February 13, 2014
- Response from Eric Rabe, Communications Counsel, Hacking Team, to Human Rights Watch, February 19, 2014

Gamma International:

- Human Rights Watch Letter to Mr. Louthean Nelson, Director, and Mr. Martin J. Muench, Gamma International, February 13, 2014
- Human Rights Watch also sent similar letters to:
    - FinFisher GmbH (former subsidiary of Gamma), February 13, 2014
    - Elaman (a retailer/distributor of Gamma/FinFisher products), February 13, 2014

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

Human Rights Watch Letter to Dr. Shiferaw Teklemariam, Minister of Federal Affairs, Government of Ethiopia

(Human Rights Watch also sent similar letters to Dr. Debretsion G. Michael, Minister of Communications and Information Technology and Dr. Getachew Ambaye, Minister of Justice)

February 11, 2014

Dr. Shiferaw Teklemariam
Minister of Federal Affairs
Ministry of Federal Affairs
PO Box 5718
Addis Ababa, Ethiopia

Re: Role of Telecommunications Vendors in Ethiopia

Dear Minister Shiferaw,

I am writing to request the government's input and perspective regarding research that Human Rights Watch is conducting on the telecommunications sector in Ethiopia.

Human Rights Watch is an independent organization that monitors and reports on human rights in more than 90 countries. We produce reports on our findings to raise awareness about human rights issues and to promote policy recommendations for change.

Since November 2012, Human Rights Watch has been researching the impact on human rights of censorship and surveillance in Ethiopia's telecommunications industry. Human Rights Watch is committed to producing material that is well-informed and objective. We hope you and your staff would be able to answer the following questions so that your views are accurately reflected in our reporting:

1. Various federal laws require warrants to be obtained prior to searches or surveillance. What directives, policies or procedures guide

judges in whether or not to grant warrants for electronic searches or surveillance? How often are court warrants obtained for electronic searches or surveillance? What regulations, policies, or procedures are in place that require security agencies or police to show the warrant to compel Ethio Telecom or other entities to assist with surveillance?

2. What policies, directives, or procedures are in place to guide intelligence gathering and surveillance that ensure rights to privacy are respected? What policies, directives, or procedures are in place to guide Ethio Telecom or Ethiopian Telecommunications Corporation (ETC) employees when they are requested by National Intelligence and Security Service (NISS) or Information Network Security Agency (INSA to access customer call records or metadata?
3. Human Rights Watch and other organizations have documented numerous cases of blocked websites, including those of opposition parties and Ethiopian news sites. On what legal basis does the Ethiopian government block websites?
4. Human Rights Watch documented the intentional jamming of numerous radio stations and television stations in apparent contravention of International Telecommunication Union (ITU) regulations. On what legal basis did Ethiopia jam these stations? Does the apparent absence of jamming since April 2013 indicate a change in policy regarding jamming by the Ethiopian government?
5. Has the Ethiopian government, Ethio Telecom or ETC ever contracted with ZTE Corporation to provide lawful intercept, deep-packet inspection, or other network filtering/management capabilities? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts. Please also describe whether such contracts were awarded as a stand-alone tender, or part of a multi-package vendor-financing contract.
6. Which government departments are authorized to engage in interception of communications, whether through ZTE's ZXMT system or some other system? What policies, procedures, and directives guide how lawful intercept systems may be used and who may be targeted?
7. Who has access to ETC customer call records and metadata? What safeguards, if any, are in place to prevent unauthorized use or disclosure of customer call records and other metadata?
8. What policies or procedures are in place to guide the government's blocking of simcards? What is the legal basis for this practice?

9. Documented evidence exists of the presence of Gamma's FinFisher on ETC servers in 2012. Is the Ethiopian government using FinFisher or has ceased use of this product? What is the legal basis for use of these surveillance tools? What laws, regulations, or policies regulate the use of FinFisher to prevent arbitrary or unlawful interference with the right to privacy?
10. Researchers at Citizen Lab analyzed and documented recent attempts by a third party to infect computers of the Ethiopian opposition in the diaspora using Hacking Team's Remote Control System or a similar system. Remote Control System is a remote surveillance tool made for government agencies that allows them to infect and monitor activity on an individual's computer or mobile device. Has Ethiopia acquired Hacking Team's Remote Control system or a similar system? Is it still currently using this or other similar software? Which one? What laws, regulations, or policies regulate the use of Remote Control System or a similar system to prevent arbitrary or unlawful interference with the right to privacy?
11. Please provide examples of any government officials including security personnel who have been investigated, suspended from duty, disciplined or prosecuted for the inappropriate acquisition and use of intercepted information.
12. Please clarify what oversight role parliamentary committees or the executive play in ensuring security and law enforcement agencies are abiding by privacy safeguards when engaging in surveillance or collecting communications data.

Thank you for your consideration and we look forward to your responses to our inquiries. We would appreciate receiving your response to this letter by March 3, 2014, to ensure that it can be reflected in our final report. Alternatively, we would greatly appreciate the opportunity to meet with you in person to discuss these questions.

Should you have any questions, please do not hesitate to contact Leslie Lefkow, Deputy Director of the Africa Division.

Sincerely,

Leslie Lefkow
Deputy Director
Africa Division

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

CC:

HUMAN RIGHTS WATCH

HRW.org

Human Rights Watch Letter to Mr. Stéphane Richard, Orange

October 28, 2013

Mr. Stéphane Richard
Chairman and Chief Executive Officer
France Telecom - Orange Group
6 Place D'Alleray
Paris, Cedex 15
France

Cc: Mr. Yves Nissim, VP, Head of Transformation and Operation in CSR
Ms. Brigitte Dumont, Director of CSR

Re: Role of Telecommunications Companies in Ethiopia

Dear Mr. Richard,

Human Rights Watch is an independent international organization that monitors human rights in more than 80 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on telecommunications companies and equipment vendors in Ethiopia.

We are drafting a report that will include a discussion of the role of telecommunications services in Ethiopia and the impact of censorship and surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We understand that France Telecom-Orange (FT) managed Ethio Telecom from 2010-2012, while also providing advice on how to modernize Ethio Telecom's management and operations. We also understand that FT has continued its relationship with Ethio Telecom for an additional year through a "support framework agreement" signed in December 2012.

We would appreciate any comments you may have about FT's business in Ethiopia, including the activities of any current and former subsidiaries. Specifically, we would appreciate responses to the following questions. This will greatly assist our understanding of FT's business in Ethiopia, its approach to human rights risk, and the legal and regulatory environment in which it works.

1. We are pleased to see FT's continued involvement in the Telecommunications Industry Dialogue and engagement with the Global Network Initiative. Please elaborate on any human rights policies and procedures it has in place to address and prevent human rights abuses associated with use of FT's services, training, or equipment. Can you describe any specific policies and procedures that apply to FT's operations in Ethiopia?
2. What human rights due diligence has FT conducted in relationship to its contracts and operations in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to FT's business in Ethiopia.
3. We understand that there is Internet censorship and the use of deep packet inspection (DPI) monitoring equipment in Ethiopia. Mr. Jean-Michel Latute, former CEO of Ethio Telecom brought in by FT, confirmed use of DPI in a statement to the press.[331] Human Rights Watch has also documented the Ethiopian government's use of counterterrorism and other security laws to censor journalists or against others who do not pose an apparent threat to national security. Has FT ever raised censorship or surveillance practices with Ethiopian authorities? What policies or procedures does FT have in place, if any, to address use of its products and services in ways that might facilitate human rights abuses?
4. Has the Ethiopian government or Ethio Telecom ever contracted with FT (or Orange University) to provide training, services, or equipment related to lawful intercept,

[331] "En Éthiopie, France Télécom accompagne la censure d'Internet," *La Croix*, October 6, 2012, http://www.la-croix.com/Actualite/Monde/En-Ethiopie-France-Telecom-accompagne-la-censure-d-Internet-_NP_-2012-06-10-816727 (accessed October 28, 2013).

DPI, or other network filtering/management capabilities? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts.

5. Has FT (or Orange University) ever provided training or consultation services to employees of the Ethiopian National and Intelligence Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature of such training or consultation? Have such services covered implementation or use of lawful intercept or DPI software and equipment?
6. We understand that Ethio Telecom uses one of ZTE Corporation's ZSmart solutions for customer billing and other purposes. To the extent possible, please describe whether and how ZSmart could be integrated and used with lawful intercept systems, either provided by ZTE or another vendor. Did FT assist with integration of ZSmart and a lawful intercept system in Ethiopia and, if so, what was the nature of the services provided?

We would appreciate a response by Friday, November 15th. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further, in person or via teleconference. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,

Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

Letter from Ms. Brigitte Dumont, Orange to Human Rights Watch

EPS/BD/Group CSR/2013.25

HUMAN RIGHTS WATCH
M Arvind Ganesan
Program Director
350 Fifth Avenue, 34th Floor
New York, NY 10118-3299

Paris, November 19, 2013

Cc : Stephane Richard, CEO Orange Group
Cynthia Wong, Senior Researcher on the Internet – HRW
Jacques Moulin, Chief Executive Officer Sofrecom
Yves Nissim, VP, Head of Transformation and Operation in CSR

Dear Mr. Ganesan,

We welcome your letter of the 29th October 2013 to Stephane Richard, CEO of the Orange Group.

Ethio Telecom is the only telecommunication operator in Ethiopia, it is fully owned by the government.
Orange and its subsidiary Sofrecom have managed Ethio Telecom from June 2010 to December 2012 through a Management Contract. The objective was to

- Create a new operator, replacing the historic operator
- Transform the organization, and the management in order for Ethio Telecom to
  - Reach world class standards
  - Provide all Ethiopian citizens with telecom services
  - Reach management autonomy by the end of the contract

Orange's role during the management contract was to transform the operator, create a commercial network and service portfolio, transfer its know-how and best practices and develop the management capacity of Ethio Telecom.
Today Orange continues to support Ethio Telecom with consultancy services. This constitutes Orange's only commitment in Ethiopia.

Point 1
Orange and its subsidiary Sofrecom's employees act according an ethical chart that was adopted by the Group in 2008. Following an external audit of its ethics program and practices, in November 2010, Sofrecom became

the first Orange Group entity to obtain an Ethics Certification by a recognized independent organization (delivered by Ethic Intelligence). Please note that Orange and Sofrecom's operations in Ethiopia started in June 2010.

Sofrecom's certification was renewed on 20th November 2012. This certification attests the compliance of Sofrecom Group practices with international ethics standards.

Among the ethical rules that constitute our chart, the following ones address specifically your concerns.

> *(extract of Sofrecom Chart of Ethics)*
> All employees shall respect local and national legislation, wherever they may be in the world. Employees shall respect the individuals and the right to protection of their private life, wherever they may be in the world. They shall thus reject all forms of discrimination and the following types of behavior:
> - moral or sexual harassment
> - behavior that is insulting, racist or violent
> - intrusive behavior in private spheres
> - casual and contemptuous behavior
> - discriminatory behavior such as that based on sex, true or alleged belonging to a race or ethnic group, sexual orientation, state of health, pregnancy or religion.

Point 2

France Telecom Orange mission in Ethiopia was and is still focused on business excellence and is performed in accordance with Orange ethic chart. If any of the activities of the Group in Ethiopia had involved a risk of human right abuse, it would have been duly reported and accordingly addressed.

Point 3

Orange has never been associated or part of the political decisions in Ethiopia concerning telecom security. Therefore neither Orange nor Sofrecom has responsibility in the selection and implementation of security equipment for Internet.
Please note that most Telcos are using DPI for controlling the bandwidth allocation in IP networks and optimizing customer experience.

Point 4

Orange, Sofrecom or Orange University have never contracted with the Ethiopian Government or Ethio Telecom to provide training, services or equipment related to lawful intercept, DPI, or other network filtering/management capabilities.

Point 5

Orange or Orange University has never provided such training or any training to the above mentioned agencies.
In order to help increase awareness on high standards used in most developed countries to fight cyber criminality Orange organized a cyber-crime workshop in Addis Ababa in 2011. This workshop was delivered by a CLUSIF representative. Please note that until 2011 Ethiopian Internet addresses were blacklisted by most of the international Internet organizations due to the high level of risk related to cyber criminality and cyber terrorism in Ethiopia.

Point 6

A Customer Care and Billing System (CCBS, the ZTE equipment in the case of Ethio Telecom), is used managing customer relationship and billing. In all cases of projects where Orange or Sofrecom is involved implement CCBS according to industry best practices ensuring the respect of necessary security rules : firewalls in order to prevent any intrusion or misuse of the system by a third party.

I reconfirm you that we are willing to cooperate with all the stakeholders, especially NGOs such as yours : remain at your disposal for any question.

Yours sincerely,

Brigitte Dumont
Chief Officer
Group Corporate Social Responsability

Human Rights Watch Letter to
Mr. Yves Nissim and Ms. Brigitte Dumont, Orange

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

December 12, 2013

Mr. Yves Nissim
VP, Head of Transformation and Operation in CSR

Ms. Brigitte Dumont
Director of CSR
France Telecom - Orange Group
6 Place D'Alleray
Paris, Cedex 15
France
Via email

Re: Follow up to November 19 letter on Ethiopia

Dear Yves and Brigitte:

Thanks again for your response to our October 29, 2013 letter "Re: Role of Telecommunications Companies in Ethiopia," as well as our meeting at the Global Network Initiative-Industry Dialogue Joint Learning Forum. We appreciate Orange's continued engagement on freedom of expression and privacy and we look forward to working with you through the GNI-ID principles working group.

I have a few follow up questions to your November 19, 2013 letter. We are committed to producing fair and objective research and we would appreciate additional information regarding the following.

In Points 1 & 2, your letter describes how Orange Group and its subsidiary Sofrecom operate in accordance with Orange's Code of Ethics and ethics chart and, accordingly, Sofrecom would have reported any risk of human right abuse it identified in Ethiopia.

The Ethiopian government has a poor human rights record with respect to freedom of expression and association, which has been well-documented.

- Does the ethics chart address conduct that impacts subscribers' right to privacy (as it relates to communications surveillance) and freedom of expression? Please describe in more detail the indicators, questions, or issues Sofrecom is instructed to examine to identify risks related to

communications privacy and freedom of expression, and steps taken to address these risks. Please describe the escalation processes used in which human rights issues are escalated by local subsidiaries to the Group level, including the circumstances that would trigger Group review.

In Point 3, your letter states that neither Orange nor Sofrecom has responsibility in the selection and implementation of security equipment for Internet networks.

- Has Orange or Sofrecom been involved in the selection or implementation of security equipment for mobile phone networks in Ethiopia? If so, please describe the nature of the equipment selected or implemented and Orange / Sofrecom's role in the process.

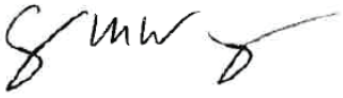
In Point 6, your letter states that where Orange or Sofrecom is involved in implementing a Customer Care and Billing System (CCBS), it does so according to industry best practice, including safeguards to prevent third party misuse or intrusion into the system.

We understand that some set of Ethio Telecom employees can access large numbers of audio recordings of subscriber phone calls through a ZSmart/ZTE CCBS system. By subscriber phone calls, we mean calls between a subscriber and a third party, but not customer support calls where Ethio Telecom was a party to a call.

- Can you confirm whether Ethio Telecom's ZTE-supplied CCBS system records subscriber phone calls or enables access to audio recordings of subscriber phone calls?
- To what extent has Orange or Sofrecom been involved in selection, implementation, or upgrading of Ethio Telecom's customer care and billing system?
- To what extent did Orange or Sofrecom discuss privacy and security practices with Ethio Telecom related to law enforcement access to subscriber communications or data?

We would appreciate any additional input or perspectives you may have. Thank you for your consideration and we look forward to your responses to our inquiries.

Sincerely,



Cynthia Wong
Senior Researcher, Internet and Human Rights
Human Rights Watch

Letter from Mr. Yves Nissim, Orange to Human Rights Watch

January 14, 2014

Points 1 &2 :

In Points 1 & 2, your letter describes how Orange Group and its subsidiary Sofrecom operate in accordance with Orange's Code of Ethics and ethics chart and, accordingly, Sofrecom would have reported any risk of human right abuse it identified in Ethiopia.

The Ethiopian government has a poor human rights record with respect to freedom of expression and association, which has been well-documented.

- Does the ethics chart address conduct that impacts subscribers' right to privacy (as it relates to communications surveillance) and freedom of expression? Please describe in more detail the indicators, questions, or issues Sofrecom is instructed to examine to identify risks related to communications privacy and freedom of expression, and steps taken to address these risks. Please describe the escalation processes used in which human rights issues are escalated by local subsidiaries to the Group level, including the circumstances that would trigger Group review.

As already stipulated the ethic chart addresses all kind of conducts that are against Orange Group ethics. The consultants are invited to refer to Orange and Sofrecom Enterprise Social Responsibility organization if they are confronted to such behaviors. Orange was managing ethio telecom, and has never been requested by the Ethiopian Government to act against ethic rules.

Orange was not up to recently facing this kind of problems. We have constructed the Telecom Industry Dialogue to try to answer the question on how to address these risks. We do have escalation processes for ethics and for Compliance. We are looking the compatibility of these escalation processes with the process needed for breaches made on freedom of speech and privacy

Point 3

In Point 3, your letter states that neither Orange nor Sofrecom has responsibility in the selection and implementation of security equipment for Internet networks.

- Has Orange or Sofrecom been involved in the selection or implementation of security equipment for mobile phone networks in Ethiopia? If so, please describe the nature of the equipment selected or implemented and Orange / Sofrecom's role in the process.

No, neither Sofrecom nor Orange have been involved in the selection or implementation of such equipment.

Point 6

In Point 6, your letter states that where Orange or Sofrecom is involved in implementing a Customer Care and Billing System (CCBS), it does so according to industry best practice, including safeguards to prevent third party misuse or intrusion into the system.

We understand that some set of Ethio Telecom employees can access large numbers of audio recordings of subscriber phone calls through a ZSmart/ZTE CCBS system. By subscriber phone calls, we mean calls between a subscriber and a third party, but not customer support calls where Ethio Telecom was a party to a call.

- Can you confirm whether Ethio Telecom's ZTE-supplied CCBS system records subscriber phone calls or enables access to audio recordings of subscriber phone calls?
- To what extent has Orange or Sofrecom been involved in selection, implementation, or upgrading of Ethio Telecom's customer care and billing system?
- To what extent did Orange or Sofrecom discuss privacy and security practices with Ethio Telecom related to law enforcement access to subscriber communications or data?

Every Customer Care and Billing System (CCBS) records the call information (calling number, called number, duration) which are information used for billing purpose. There is no need to record the calls and this is the only usage that Orange / Sofrecom are aware of.

Orange/Sofrecom was not involved in the selection of ethio telecom CCBS. Orange Sofrecom has participated in the CCBS implementation and has made sure that it was done according to industry best practices ensuring the respect of necessary security rules and firewalls in order to prevent any intrusion or misuse of the system by a third party. Orange and Sofrecom have not been involved in any discussion with the Ethiopian government concerning law enforcement access to subscriber communication or data.

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

Human Rights Watch Letter to Mr. Eric Xu, Huawei

October 29, 2013

Mr. Eric Xu
Acting CEO
Huawei
Huawei Industrial Park
Bantian, Longgang District
Shenzhen, Guangdong
People's Republic of China, 518129

Cc: Mr. Deng Biao, Chairman of the Corporate Sustainable Development Committee
Mr. William Plummer, Vice President, External Affairs

Re: Role of Telecommunications Companies in Ethiopia

Dear Mr. Xu,

Human Rights Watch is an independent international organization that monitors human rights in more than 80 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on the role of telecommunications equipment companies in Ethiopia.

We are drafting a report that will include a discussion of the role of Huawei in Ethiopia and the impact of surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We would appreciate any comments you may have about Huawei's business in Ethiopia, including the activities of any current and former

subsidiaries. Specifically, we would appreciate responses to the following questions. This will greatly assist our understanding of Huawei, the products and solutions it offers, its approach to human rights risk, and the legal and regulatory environment in which it works.

1. Can Huawei elaborate on any human rights policies and procedures it has in place to address and prevent human rights abuses associated with use of its services or equipment? Can you describe any specific policies and procedures that apply to Huawei's operations in Ethiopia?
2. Has Huawei ever conducted human rights due diligence in relationship to its contracts and operations in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to Huawei's business in Ethiopia.
3. We understand that there is Internet censorship and the use of deep packet inspection (DPI) monitoring equipment in Ethiopia. Human Rights Watch has also documented the Ethiopian government's use of counterterrorism and other security laws to censor journalists or against others who do not pose an apparent threat to national security. Has Huawei ever raised censorship or surveillance practices with Ethiopian authorities? What policies or procedures does Huawei have in place, if any, to address use of its products and services in ways that might facilitate human rights abuses?
4. Has the Ethiopian government or Ethio Telecom/Ethiopian Telecommunications Corporation (ETC) ever contracted with Huawei to provide lawful intercept, DPI, or other network filtering/management capabilities? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts. Please also describe whether such contracts were awarded as a stand-alone tender, or part of a multi-package vender-financing contract.
5. Has Huawei ever provided training or consultation services to employees of Ethio Telecom/ETC or Ethiopian government employees on use of lawful intercept, DPI, or other network filtering/management equipment or software, whether provided by Huawei or another vendor? If so, please describe the nature and scope of services provided.
6. Has Huawei ever provided training or consultation services to the Ethiopian National Intelligence and Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature and scope of such training or consultation? Have such services covered implementation or use of lawful intercept or DPI software and equipment?

We would appreciate a response by Friday, November 15th. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,

Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

Letter from Mr. William Plummer, Huawei to Human Rights Watch

November 12, 2013

Mr. Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch
1630 Connecticut Avenue, Ste. 500
Washington DC, 20009

Dear Mr. Ganesan:

I am writing to respond to your email communication dated October 29, 2013, addressed to Mr. Xu, Mr. Deng and myself.

With respect to the questions raised, Huawei respectfully offers the following clarifications:

As a $35 billion dollar world-leading multinational company doing business in almost 150 markets across the globe, Huawei complies with all applicable laws and regulations regarding the protection of human rights. Huawei takes a global approach to business, adhering to common Business Conduct Guidelines in all the markets in which we do business. We are not aware of any case in which human rights abuses have been associated with the use of Huawei services or equipment.

Huawei's Business Conduct Guidelines clearly state that "Huawei will never tolerate misuse of information and telecommunication technology to conduct surveillance on end users' communications and / or movements, or to block or disrupt communications, or to restrict the free flow of unbiased information." Furthermore, we can confirm that we have never been asked to provide access to our technology or to provide any data or information on any citizen or organization to any Government, or their agencies.

Like our global peers supplying telecom network solutions, Huawei builds to globally-standardized specifications, including, for instance, the requirement to build into our solutions an interface for lawful intercept capabilities. Notably, Huawei does not develop or deliver actual lawful intercept solutions.

Similarly, like our global peers, Huawei has, according to 3GPP, ITU-T and other open standards, developed network management solutions that help our customers analyze data in their networks, such as protocol/application identification, URL categorization, etc. which enable network operators to optimize their networks. These solutions cannot monitor the content of Internet communications. We do provide training related to the operation and maintenance of such equipment.

Further information about Huawei and our company and policies – as well as our informative Annual Report - is available at www.huawei.com/en/about-Huawei/corporate-info/index.htm. We are certainly open to further conversation on any matters of interest to your organization.

Very best regards,

William B. Plummer
Vice President, External Affairs
Huawei Technologies
875 15th Street, NW, Ste. 825
Washington, DC 20005

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

Human Rights Watch Letter to Sinovatio

October 29, 2013

Sinovatio
ZTEsec Plaza
No.888 Zhengfang Road
Jiangning District
Nanjing, People's Republic of China, 211153

Dear Sir/Madam,

Human Rights Watch is an independent international organization that monitors human rights in more than 80 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on the role of telecommunications equipment companies in Ethiopia.

We are drafting a report that will include a discussion of ZTESec's/Sinovatio's business in Ethiopia and the impact of surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We would appreciate any comments you may have about Sinovatio's business in Ethiopia, including activities conducted while a subsidiary of ZTE Corporation (for example, while operating as Shenzhen ZTE Special Equipment Company Ltd or Nanjing ZTE Special Software Company Ltd). Specifically, we would appreciate responses to the following questions. This will greatly assist our understanding of Sinovatio, the products and solutions it offers, its approach to human rights risk, and the legal and regulatory environment in which it works.

1. Can Sinovatio elaborate on any human rights policies and procedures it has in place to address and prevent human rights abuses

associated with use of Sinovatio's services or equipment? Can you describe any specific policies and procedures that apply to Sinovatio's operations in Ethiopia?

2. Has Sinovatio ever conducted human rights due diligence in relationship to its contracts and operations in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to Sinovatio's business in Ethiopia.
3. We understand that there is Internet censorship and the use of deep packet inspection (DPI) monitoring equipment in Ethiopia. Human Rights Watch has also documented the Ethiopian government's use of counterterrorism and other security laws to censor journalists or against others who do not pose an apparent threat to national security. Has Sinovatio ever raised censorship or surveillance practices with Ethiopian authorities? What policies or procedures does Sinovatio have in place, if any, to address use of its products and services in ways that might facilitate human rights abuses?
4. Has the Ethiopian government or Ethio Telecom/Ethiopian Telecommunications Corporation (ETC) ever contracted with Sinovatio to provide lawful intercept, DPI, or other network filtering/management capabilities? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts. Please also describe whether such contracts were awarded as a stand-alone tender, or part of a multi-package vendor-financing contract.
5. Specifically, has Ethio Telecom/ETC, the Information Network Security Agency, or any other government agency contracted with Sinovatio (or ZTE Corporation) to purchase ZTE's ZXMT lawful intercept solution? If so, when was the system installed? Did Sinovatio customize installation or training for this product at the request of government agencies or Ethio Telecom/ETC, and how?
6. We understand that Ethio Telecom uses one of ZTE's ZSmart solutions for customer billing and other purposes. Please describe whether and how ZSmart can be used to record and store the content of phone calls. In addition, please describe whether and how ZSmart could be integrated and used with other lawful intercept systems, either provided by Sinovatio or another vendor. Did Sinovatio assist with integration of ZSmart and a lawful intercept system in Ethiopia and, if so, what was the nature of the services provided?

7. Has Sinovatio ever provided training or consultation services to employees of Ethio Telecom/ETC or Ethiopian government employees on use of lawful intercept, DPI, or other network filtering/management equipment or software, whether provided by Sinovatio or another vendor? If so, please describe the nature and scope of services provided.
8. Has Sinovatio ever provided training or consultation services to the Ethiopian National Intelligence and Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature and scope of such training or consultation? Have such services covered implementation or use of lawful intercept or DPI software and equipment?
9. To what extent is Sinovatio subject to China's State-owned Assets Supervision and Administration Commission (SASAC) oversight and how often have you reported to SASAC? Have you ever been sanctioned by SASAC? If so, please describe the circumstances.

We would appreciate a response by Friday, November 15th. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,

Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

Human Rights Watch Letter to Mr. Shi Lirong, ZTE

October 29, 2013

Mr. Shi Lirong
President and Executive Director
ZTE Corporation
No. 55, Hi-tech Road South
Shenzhen, Guangdong Province
People's Republic of China, 518057

Cc: Mr. David Dai Shu, Director of Global Public Affairs
Ms. Margrete Ma, Public Relations Spokesperson

Re: Role of Telecommunications Companies in Ethiopia

Dear Mr. Shi Lirong,

Human Rights Watch is an independent international organization that monitors human rights in more than 80 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on the role of telecommunications equipment companies in Ethiopia.

We are drafting a report that will include a discussion of ZTE Corporation's business in Ethiopia and the impact of surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We would appreciate any comments you may have about ZTE's business in Ethiopia, including the activities of ZTE's current and former subsidiaries. Specifically, we would appreciate responses to the following questions. This will greatly assist our understanding of ZTE, the products and

solutions it offers, its approach to human rights risk, and the legal and regulatory environment in which it works.

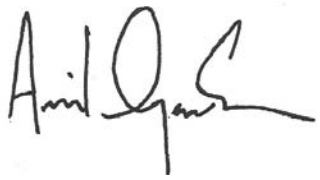
1. Can ZTE elaborate on any human rights policies and procedures it has in place to address and prevent human rights abuses associated with use of ZTE's services or equipment? Can you describe any specific policies and procedures that apply to ZTE's operations in Ethiopia?
2. Has ZTE ever conducted human rights due diligence in relationship to its contracts and operations in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to ZTE's business in Ethiopia.
3. We understand that there is Internet censorship and the use of deep packet inspection (DPI) monitoring equipment in Ethiopia. Human Rights Watch has also documented the Ethiopian government's use of counterterrorism and other security laws to censor journalists or against others who do not pose an apparent threat to national security. Has ZTE ever raised censorship or surveillance practices with Ethiopian authorities? What policies or procedures does ZTE have in place, if any, to address use of its products and services in ways that might facilitate human rights abuses?
4. Has the Ethiopian government or Ethio Telecom/Ethiopian Telecommunications Corporation (ETC) ever contracted with ZTE to provide lawful intercept, DPI, or other network filtering/management capabilities? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts. Please also describe whether such contracts were awarded as a stand-alone tender, or part of a multi-package vendor-financing contract.
5. Specifically, has Ethio Telecom/ETC, the Information Network Security Agency, or any other government agency contracted with ZTE to purchase ZTE's ZXMT lawful intercept solution? If so, when was the system installed? Did ZTE customize installation or training for this product at the request of government agencies or Ethio Telecom/ETC, and how?
6. We understand that Ethio Telecom uses one of ZTE's ZSmart solutions for customer billing and other purposes. Please describe whether and how ZSmart can be used to record and store the content of phone calls. In addition, please describe whether and how ZSmart could be integrated and used with other lawful intercept systems, either provided by ZTE or another vendor. Did ZTE assist with integration of ZSmart and a lawful intercept system in Ethiopia and, if so, what was the nature of the services provided?

7. Has ZTE (or ZTE University) ever provided training or consultation services to employees of Ethio Telecom/ETC or Ethiopian government employees on use of lawful intercept, DPI, or other network filtering/management equipment or software, whether provided by ZTE or another vendor? If so, please describe the nature and scope of services provided.
8. Has ZTE (or ZTE University) ever provided training or consultation services to the Ethiopian National Intelligence and Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature and scope of such training or consultation? Have such services covered implementation or use of lawful intercept or DPI software and equipment?
9. To what extent is ZTE subject to China's State-owned Assets Supervision and Administration Commission (SASAC) oversight and how often have you reported to SASAC? Have you ever been sanctioned by SASAC? If so, please describe the circumstances.

We would appreciate a response by Friday, November 15th. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,



Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

Human Rights Watch Letter to Mr. David Vincenzetti and Mr. Valeriano Bedeschi, Hacking Team

HUMAN RIGHTS WATCH

HRW.org

February 13, 2014

Mr. David Vincenzetti and Mr. Valeriano Bedeschi
Hacking Team (HT S.r.l.)
Via della Moscova n.13
20121 - Milano
Italy

Cc: Mr. Eric Rabe

Re: Sale and Use of Hacking Team Solutions in Ethiopia

Dear Mr. Vincenzetti and Mr. Bedeschi:

Human Rights Watch is an independent international organization that monitors human rights in more than 90 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on the role of technology companies in Ethiopia.

We are drafting a report that will include a discussion of the possible use of Hacking Team products by Ethiopian authorities and the impact of surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We would appreciate any comments you may have about Hacking Team's business in Ethiopia, including the activities of any current and former subsidiaries or resellers. Specifically, we would appreciate responses to the following questions. This will greatly assist our understanding of

Hacking Team, the products and solutions it offers, its approach to human rights risk, and the legal and regulatory environment in which it works.

1. Aside from the firm's published "Customer Policy,"[332] please elaborate on any human rights policies and procedures Hacking Team has in place to address and prevent human rights abuses linked with use of its products or services.
2. To what extent do your Customer Policy or other human rights policies and procedures address the actions of your distributors, resellers, or other business partners? Please describe what, if any, human rights responsibilities your policies and procedures impose on your distributors, resellers, or other business partners.
3. Hacking Team's Customer Policy states that through contract, the company "requires customers to abide by applicable law" and that Hacking Team will not sell or provide support to governments who "refuse to sign contracts that include requirements that [Hacking Team] software be used lawfully."[333] Please describe the specific laws (or specific categories of law) Hacking Team requires customers to abide by. Do the applicable laws also include a government's obligations under international human rights law?
4. Hacking Team's Customer Policy states that the company will not sell or provide technical support to governments who "refuse to agree to or comply with provisions in [its] contracts that describe the intended use of [Hacking Team] software."[334] When negotiating a contract for goods or services, to what extent does Hacking Team or its resellers inquire about the end use or end users of its products and services? What are the allowable end uses described in Hacking Team contracts?
5. Hacking Team's Customer Policy states that if the company suspends support for its technology, the "product soon becomes useless."[335] Hacking Team has also stated in its policy and in media reports that Hacking Team products include a mandatory "auditing feature" that allows agency officials or other administrators to monitor and

[332] Hacking Team, "Customer Policy," 2013, http://www.hackingteam.it/index.php/customer-policy (accessed February 12, 2014).

[333] Ibid.

[334] Ibid.

[335] Ibid.

identify unauthorized use of the tool.[336] How does Hacking Team monitor whether customers are complying with the terms of their contracts or otherwise using Hacking Team products to facilitate human rights abuses? To what extent can Hacking Team monitor who may be being targeted with its remote infection or intrusion tools?

6. Researchers at Citizen Lab have documented phishing attacks directed at employees of Ethiopian Satellite Television (ESAT), an independent, diaspora-run satellite television station. These attacks involved spyware that matched previously established characteristics of Hacking Team's Remote Control System identified by Citizen Lab.[337] Has the Ethiopian government or Ethio Telecom/Ethiopian Telecommunications Corporation (ETC) ever contracted with Hacking Team to provide lawful intercept, IT intrusion, or remote monitoring and infection solutions? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts.
7. Has Hacking Team ever conducted human rights or Know-Your-Customer due diligence in relationship to sales (potential or completed) in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to use of Hacking Team's products in Ethiopia or by Ethiopian authorities. Can you describe any specific human rights policies and procedures that apply to Hacking Team's business in Ethiopia?
8. Hacking Team's Customer Policy states that in reviewing potential customers before a sale, it examines the "potential customer's laws, regulations, and practices regarding surveillance," as well as credible third party reports about the risk of human rights abuses by the potential customer. Human Rights Watch has documented the Ethiopian government's use of counterterrorism and other security laws against journalists or others who do not pose an apparent threat to national security.[338] If Hacking Team has engaged the government about its products and services, to what extent has Hacking

---

[336] Ibid; David Gilbert, "Hacking Team and the Murky World of State-Sponsored Spying," *International Business Times*, March 13, 2013, http://www.ibtimes.co.uk/hacking-team-murky-world-state-sponsored-spying-445507.(accessed February 12, 2014).

[337] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists (accessed February 12, 2014).

[338] See, for example, Human Rights Watch, *"One Hundred Ways of Putting Pressure": Violations of Freedom of Expression and Association in Ethiopia*, March 2010, http://www.hrw.org/reports/2010/03/24/one-hundred-ways-putting-pressure-o and "Stop Using anti-Terror Law to Stifle Peaceful Dissent," Human Rights Watch news release, November 21, 2011, http://www.hrw.org/news/2011/11/21/ethiopia-stop-using-anti-terror-law-stifle-peaceful-dissent.

Team ever raised illegal surveillance practices or misuse of lawful intercept/monitoring technology with Ethiopian authorities?

9. Has Hacking Team ever suspended support for any products or services in Ethiopia?
10. Has Hacking Team ever provided training or consultation services to employees of Ethio Telecom/ETC or Ethiopian government employees on use of lawful intercept, IT intrusion, or remote monitoring and infection solutions? If so, please describe the nature and scope of services provided.
11. Has Hacking Team ever provided training or consultation services to the Ethiopian National Intelligence and Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature and scope of such training or consultation? Have such services covered implementation or use of lawful intercept, intrusion, or remote monitoring solutions?

We would appreciate a response by February 28, 2014. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,

Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

Email Response from Eric Rabe, Hacking Team to Human Rights Watch

Hi, Cynthia,

I serve as communications counsel to Hacking Team. As the company has developed over the last several years, I have worked with Hacking Team to answer media questions and to develop public policies.

We have received your letter. As I think you know, our statement regarding most of the information you request can be found on our website under Customer Policy. Hacking Team believes this Customer Policy is the most extensive declaration by any company in the lawful surveillance industry of the expectations of a service provider regarding the conduct of clients.

Despite the skepticism of some in the activist community, Hacking Team makes a diligent effort to assure that HT tools are not abused or misused. As we make clear in our Customer Policy statement, we expect our clients to behave responsibly and within the law as it applies to them. Obviously, Hacking Team is not itself a law enforcement agency. However, when questions about the proper use of our tools are raised either internally or come to our attention from outside the company, we investigate. We can and we have suspended support for our software in cases where we believed an agency has misused or may misuse the software. When we do that, the software becomes vulnerable to detection and therefore useless. We have refused to do business with prospective clients for the same reason.

Of course, to be effective for legitimate law enforcement investigations, the agencies using the software HT provides must be able to conduct confidential investigations. It is they, not Hacking Team, that operate the software in the course of those investigations. In order to maintain their confidentiality, we do not confirm or deny the existence of any individual customer or their country location.

Hope that is helpful,

Eric

Eric Rabe

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

Human Rights Watch Letter to Mr. Louthean Nelson and Mr. Martin J. Muench, Gamma International

(Human Rights Watch also sent similar letters to FinFisher GmbH and Elaman GmbH)

HUMAN RIGHTS WATCH

HRW.org

February 13, 2014

Mr. Louthean Nelson and Mr. Martin J. Muench
Gamma International
Fellows House
46 Royce Close
West Portway Industrial Estate
Andover
Hants SP10 3TX
United Kingdom

Re: Sale and Use of Gamma/FinFisher Solutions in Ethiopia

Dear Mr. Nelson and Mr. Muench:

Human Rights Watch is an independent international organization that monitors human rights in more than 90 countries around the world. I am writing to request your input and perspective regarding research that Human Rights Watch is conducting on the role of technology companies in Ethiopia.

We are drafting a report that will include a discussion of the possible use of Gamma International's FinFisher products by Ethiopian authorities and the impact of surveillance on human rights. It is our goal to present a thorough and objective report. To that end, we are soliciting information and views from your company.

We would appreciate any comments you may have about Gamma's business in Ethiopia, including the activities of any current and former subsidiaries or resellers. Specifically, we would appreciate responses to

the following questions. This will greatly assist our understanding of Gamma, the products and solutions it offers, its approach to human rights risk, and the legal and regulatory environment in which it works.

1. Can Gamma elaborate on any human rights policies and procedures it has in place to address and prevent human rights abuses linked with use of its products or services?
2. To what extent do your human rights policies and procedures address the actions of your distributors, resellers, or other business partners? Please describe what, if any, human rights responsibilities your policies and procedures impose on your distributors, resellers, or other business partners.
3. When negotiating a contract for products or services, to what extent does Gamma or its resellers inquire about the end use or end users of its products and services? To what extent does Gamma review local laws and practices and third party reports on a prospective customer's human rights record before completing a new sales or service contract?
4. Has the Ethiopian government or Ethio Telecom/Ethiopian Telecommunications Corporation (ETC) ever contracted with Gamma to provide lawful intercept, IT intrusion, or remote monitoring and infection solutions? If so, please describe the nature of the services, software or equipment provided, their capabilities, and the dates of relevant contracts.
5. Has Gamma ever provided training or consultation services to employees of Ethio Telecom/ETC or Ethiopian government employees on use of lawful intercept, IT intrusion, or remote monitoring and infection solutions? If so, please describe the nature and scope of services provided.
6. Has Gamma ever provided training or consultation services to the Ethiopian National Intelligence and Security Services, Information Network Security Agency, federal or regional police, or Ethiopian Defense Forces? If so, what was the nature and scope of such training or consultation? Have such services covered implementation or use of lawful intercept, intrusion, or remote monitoring solutions?
7. Has Gamma ever conducted human rights due diligence (or other human rights review) in relationship to a potential or finalized transaction in Ethiopia? If so, please describe the findings and steps taken, if any, to prevent or address human rights abuses linked to use of Gamma's products in Ethiopia or by Ethiopian

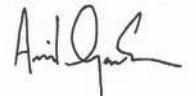
authorities. Can you describe any specific human rights policies and procedures that apply to Gamma's business in Ethiopia?

8. Human Rights Watch has documented the Ethiopian government's use of counterterrorism and other security laws against journalists or others who do not pose an apparent threat to national security. To the extent Gamma has engaged the government about its products and services, has Gamma ever raised illegal surveillance practices or misuse of lawful intercept/monitoring technology with Ethiopian authorities?
9. What policies or procedures does Gamma have in place, if any, to prevent use of its products and services in ways that might facilitate human rights abuses? For example, to what extent does Gamma place limits on the end uses or end users of FinSpy through licensing or other agreements (other than restricting the number of simultaneous targets)?
10. To what extent can Gamma monitor who may be being targeted with its remote infection or intrusion tools?
11. What policies or procedures does Gamma have in place, if any, to stop misuse of its products and services when uncovered? For example, does Gamma incorporate end use clauses in contracts that would enable Gamma to terminate a contract if its equipment or software is being misused to facilitate human rights abuses?

We would appreciate a response by February 28, 2014. If we do not receive a reply by then, we may be unable to include information you provide in our published report.

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact our Senior Internet Researcher, Ms. Cynthia Wong.

Sincerely,



Arvind Ganesan
Director, Business and Human Rights Program
Human Rights Watch

“They Know Everything We Do”

Telecom and Internet Surveillance in Ethiopia

Ethiopia’s Internet and telecommunications sector is rapidly growing, with significant implications for freedom of expression, access to information, and economic development. But the Ethiopian government’s efforts to control the sector may undermine those potential benefits. Technology developed by Chinese companies allows the government to access mobile phone records and call recordings without adequate protections for the right to privacy. The government is using some of the world’s most sophisticated surveillance malware, provided by European companies, to monitor the activities of the diaspora.

“They Know Everything We Do”: Telecom and Internet Surveillance in Ethiopia documents how Ethiopia’s government uses its control over the telecom system to restrict individuals’ rights. Based on over 100 interviews with victims of government abuses, former government officials, and former staff of telecom companies, the report describes the various methods used by Ethiopian authorities to monitor individuals and inhibit their activities online.

Individuals with perceived or tenuous connections to opposition groups are arbitrarily arrested and interrogated based on their phone calls. Security agencies rarely acquire warrants, despite the legal requirement to obtain them in most circumstances. Government censors routinely block websites of opposition groups and independent media, while bloggers and social media users face harassment and the threat of arrest should they refuse to tone down their writings.

Human Rights Watch calls on the government of Ethiopia to enact appropriate rights protections and review the conduct of government agencies tasked with surveillance. European governments should regulate the export of surveillance tools by companies within their jurisdiction to prevent abuse of these technologies by repressive governments.

Internet café in Lalibela, Amhara Region, Ethiopia.

© 2010 Hemis.fr/AFP Photo

hrw.org