Article

Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia

Daniel Grinberg

University of California, Santa Barbara, US.
dgrinberg@umail.ucsb.edu

Abstract

This article explores how authoritarianism in Ethiopia is constraining its citizens' ranges of political and digital expression. With a state monopoly on digital services, the country has lower rates of internet and mobile phone access than many of its African counterparts. However, to reach its ambitious plan for national development, Ethiopian officials are increasingly deploying surveillance to mitigate the problem I refer to as the "Authoritarian Dilemma." Through more flexible modes of control like pervasive monitoring, intimidation, and targeted censorship, the one-party state is seeking to simultaneously promote growth and stifle digital dissent. I outline some of the methods and logics that the government is using to pursue these objectives. Yet, as I argue, the chilling effects of surveillance in Ethiopia also damage the prospects for sustainable development and further marginalize the voices of political challengers and critics.

Introduction

In October 2016, Ethiopian Prime Minister Hailemariam Desalgn declared a nationwide six-month state of emergency. This crackdown was precipitated by police officers using tear gas against protesters at a cultural festival and triggering a stampede that killed over fifty people (Schemm 2016). The situation escalated as citizens attacked state-owned and foreign factories and organized anti-government protests. As the government sharply curtailed the right to free assembly, security forces detained tens of thousands of Ethiopians and conducted warrantless searches of their homes (Schemm 2017). The state authorities also blocked social media access, and intensified the practice of internet censorship. By March 2017, the parliament had used the ongoing unrest in the country to justify unanimously extending the state of emergency another four months (Schemm 2017).

Unfortunately, such limits on embodied and digital freedoms are merely an escalation of the rigorous security measures that Ethiopians have long faced. The situation is even more dire for groups like activists, journalists, minority groups, opposition party members, and expatriates who risk threats like detention and torture. Authorities have also subjected these vulnerable groups to targeted embodied and digital surveillance to further stymie their abilities to communicate, organize, and dissent. This expansion of control has exacerbated the already-deep divisions in Ethiopian society and heightened the culture of fear and paranoia among citizens.

In the following article, I will first historically situate the country's contemporary state of political and digital authoritarianism. I will then underscore the various methods and scales of digital surveillance that

Grinberg, Daniel. 2017. Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia. *Surveillance & Society* 15(3/4): 432-438.

<http://library.queensu.ca/ojs/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2017 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#).

the state has deployed to calcify its grip on power. Through this discussion, I will also extrapolate on the “Authoritarian Dilemma” and its implications for surveillance. Such an intervention is significant, because it emphasizes a milieu that surveillance studies still too often effaces. Despite the rightful shift away from assumptions of a universal subject, the scholarship in the field largely continues to come from Western and developed nations and centralize those perspectives. The Ethiopian context provides an opportunity to think through other crucial distinctions, such as the differing manifestations of rural and urban surveillance, the legacies of military coups and civil wars, and the comparative parallels and disjunctures emerging across sub-Saharan Africa. Here, my discussion foregrounds another under-recognized issue by asking how digital monitoring and suppression transpire differently in a developing nation with relatively low digital access. It will also raise complementary concerns that warrant further analysis, such as the impacts of telecom monopolization and foreign companies’ prominent role in propelling African state surveillance.

Political and Digital Authoritarianism

Home to about 102 million people, Ethiopia is the second most populous nation in Africa. Though it is the oldest independent nation on the continent, it has faced numerous violent transitions of power and internal turmoil throughout the 20th century. In 1974, the Marxist Derg regime orchestrated a military coup and seized control from Emperor Haile Selassie (Adejumobi 2007: 119). Under the Soviet-supported rule of military dictator Mengistu Haile Mariam, the country became a one-party state. To quash the challenge of opposition parties like the communist Ethiopian People’s Revolution Party (EPRP), the Derg government unleashed the brutal Red Terror genocide that killed tens of thousands of people (Toggia 2012: 273-274). After a three-year famine killed another million Ethiopians and the fall of the Soviet Union, another rebel group, the Ethiopian People’s Revolutionary Democratic Front (EPRDF), finally overthrew Mengistu in 1991 (Adejumobi 2007: 128).

Although the EPRDF established a parliamentary republic of “revolutionary democracy,” subsequent elections have predominantly strengthened the ruling party’s power. Opposition party members and international observers have criticized both the 2000 and 2005 elections, which officially secured a strong EPRDF majority. In the latter case, suspicious voting results prompted widespread accusations of fraud and public demonstrations (Freedom House 2008). Security forces responded by killing 42 protesters and arresting over 4,000 people, including opposition leaders. Further cracking down on civil liberties, the government banned protests and put opposition leaders, human rights activists, and journalists on trial for constitutional crimes (Freedom House 2008). One disproportionately targeted group has been the ethnic Oromo population, which constitutes a majority of the population at 34 per cent but has disproportionately little political power. Attempting to forestall electoral challenges, the EPRDF has used the insurgent group Oromo Liberation Front (OLF)’s violent resistance to justify its broader repression of the Oromo people (Human Rights Watch 2014: 1). In the 2010 and 2015 elections, the EPRDF again exercised an array of repressive practices to fortify its control. In the former contest, the party and its regional allies won all but one of 546 parliamentary seats; in the latter, the party even claimed this last seat (Winsor 2015).

In light of such disconcerting developments, the Economist Intelligence Unit ranked Ethiopia the 125th most democratic nation out of 167 nations in its 2016 Democracy Index (2017: 10). Like 50 other countries that year, its lack of electoral pluralism, political participation, and civil liberties qualified it as an authoritarian regime. Furthermore, indicating the decline of democratic protections, the 2016 report gave Ethiopia its lowest score to date since the Index began in 2006 (Economist Intelligence Unit 2017: 29). Similarly, Freedom House, an independent advocacy organization focused on global rights, categorized Ethiopia as Partly Free in 2006 (Freedom House 2007) and in its lowest classification, Not Free, in 2016 (Freedom House 2017a).

As the country's political landscape has shifted, the growing centrality of information and communication technologies (ICTs) has aggravated the problem often referred to as the "Dictator's Dilemma."^{1 2} (In the case of this regime, the "Authoritarian Dilemma" would be a more accurate term.³) This quandary presents authoritarian governments with the choice between increasing digital freedoms that can facilitate national development and participation in the global information economy, and restricting digital freedoms to try to tamp down internal dissent and preserve the regime's power. As the Ethiopian case and others illustrate, the legal, economic, and technological responses to the dilemma can yield especially formative consequences for developing nations.

To date, the EPRDF has primarily opted to restrict rights and adopt what scholars call "digital authoritarianism" (Erixon and Lee-Makiyama 2011) or "networked authoritarianism" (MacKinnon 2011). The country's sole telecommunications service provider, Ethio Telecom, is state-owned and controls all access to phone and internet networks. The government can determine which websites and services to censor, and when to obstruct access altogether. Although most radio and television stations are already affiliated with the government, it can also jam signals to block objectionable content from airing (Human Rights Watch 2014: 82). Thus, the state's monopolization of information and communications technologies (ICTs) and media channels has become another key means of augmenting its authority.

Yet, this maintenance of state control is partly responsible for Ethiopia having far lower rates of digital adoption than its neighbors. As of 2015, 11.6 per cent had some level of access, while only 0.75 per cent did in 2010. By comparison, Kenya, which has been nicknamed the Silicon Savannah, had rates of 45.6 per cent in 2015 and 14 per cent in 2010 (International Telecommunication Union 2016). Ethiopia has struggled to adequately expand the technical infrastructure to reach the 80 per cent of residents who live in rural areas (World Bank n.d.). While the state has enlisted the services of Chinese telecom firms Huawei and ZTE and Swedish firm Ericsson, the rural infrastructure remains underdeveloped (Solomon 2014). This setback has compounded other contributing factors of diminished access, like the prohibitive cost of broadband, inferior connectivity speeds and network coverage, and propensity for outages.

Amid its ambitious plan for national growth, the Ethiopian government continues to grapple with the Authoritarian Dilemma (Federal Democratic Republic of Ethiopia 2016).⁴ To promote higher rates of digital adoption, it is increasingly enacting what Ronald Deibert and Rafal Rohozinski refer to as "next-generation techniques" of control (2010: 6). Deibert and Rohozinski describe these alternatives to the widespread denial of digital access as "more subtle, flexible, and even offensive in character" (2010: 6). For the EPRDF, the intensification of surveillance is one such mechanism of control. While surveillance does not supplant internet filtering and operates alongside it, the multiscalar enactments of monitoring arguably authorize the expansion of digital usage. Paradoxically though, the prevalence of surveillance is also a substantial hindrance to the adoption and use of digital technologies in Ethiopia. Because of the covert, unpredictable

¹ The term "dictator's dilemma" comes from Christopher Kedzie (see Kedzie 1997). Kedzie draws on a 1985 speech on totalitarian societies by then-U.S. Secretary of State George Schultz and credits Larry Press for coining the term "dictator's dilemma" during a private conversation.

² For an in-depth analysis of this conundrum, see Jaclyn Kerr's (2014) paper, "The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States."

³ Nivien Saleh uses the case study of the 2011 Egyptian uprising to argue that the term "Dictator's Dilemma" wrongly attributes authoritarian power to an individual (Saleh 2012: 481). Hence, I use the alternative and more accurate term "Authoritarian Dilemma."

⁴ In its Growth and Transformation Plan for the timespan between 2015-2016 and 2010-2020, the Ethiopian government sets lofty goals for ICT use and digital expansion. It seeks to grow from 9.4 million internet subscribers, 43.9 per cent mobile phone coverage, and 1.59 million broadband data service and internet subscribers in 2014/2015 to 56 million internet subscribers, 100 per cent mobile coverage, and 39.1 million broadband subscribers in 2019/2020 (Federal Democratic Republic of Ethiopia 2016: 96).

nature of surveillance, both its real and perceived abuses meaningfully chill the ranges of self-expression and communication. State incursions also obstruct the flows of domestic and global information exchange, accelerate social divisions among citizens, and ultimately restrict the full capacity of sustainable development.

Digital Surveillance in Practice

All digital users in Ethiopia are under surveillance to some degree. Because the state has monopolized internet access and controls the telecom infrastructure, intelligence agencies maintain the ability to opaquely monitor the country's residents online. In moments of unrest, the mass tracking of digital communications intensifies and often precipitates the shutdown of social networks or full internet and mobile access. In addition to such broad applications of digital surveillance, police and government agents disproportionately target populations that they consider a challenge to the EPRDF's unilateral authority. This narrower, more forceful attention directed against people like opposition party members, critics, journalists, and ethnic Oromo can be coupled with threats, arrests, torture, and imprisonment.

To acknowledge these multifaceted gradations of digital surveillance, this section will first discuss a few of the regime's broadly directed practices. It will then detail a few of the practices that selectively target oppositional groups. Due to limitations on space, neither discussion can fully account for the multitude of practices that are occurring in Ethiopia. Rather, they intend to identify some of the concurrent scales, technologies, and agents at work and to elaborate the stakes of the Authoritarian Dilemma in developing nations. This discussion also seeks to affirm the need for more comprehensive scholarly exploration of digital surveillance in this national and regional context.

Many of the most invasive instantiations of surveillance in Ethiopia center on mobile phones. Like over 40 other African countries (Nyst 2012), Ethiopian policy requires customers to present identification and submit a photograph and personal information to purchase a SIM card (Freedom House 2017b: 15). This process alerts users that their communication practices will make them identifiable, and invariably chills the willingness to discuss sensitive issues on the phone.⁵ Upon activating their SIM cards, users in the country become even easier to monitor. According to a Human Rights Watch report, "[T]he 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" (2014: 34). The state can also limit or block landline and mobile phone access during politically sensitive moments (Shaban 2016). Because users predominantly access the internet through their mobile phones, the shutdown of mobile networks serves a potent dual function of censorship.

As internet cafés gain popularity in urban areas, the government is also scrutinizing these locations more intensely. Here, too, it is attempting to strike an uneasy balance between granting measured access to a greater number of users and exerting full control. The state's primary concern is that the shared computers can anonymize users and enable critics to gather and distribute information in more secure settings. The cafés are subject to many onerous requirements, such as a complex, months-long screening process required to obtain an operator's license and a ban on Voice over Internet Protocol (VoIP) (Freedom House 2017b: 6). Operators have also reported the use of varying enforcement and intimidation tactics. In interviews with Human Rights Watch, one operator stated that an official ordered him to make every monitor simultaneously visible and to report any suspicious behavior (2014: 67). Another operator said that officials threatened to confiscate her equipment and imprison her, because a customer had accessed online material that criticized

⁵ For more on the political and social implications of mandatory SIM registration in Africa, see Kevin P. Donovan and Aaron K. Martin (2014).

the government. Other officials have demanded details on specific users and the sites they visited and have themselves monitored cafes in plainclothes disguises (Human Rights Watch 2014: 67).

Agencies like the Ministry of Communications and Information Technology (MCIT) and the Information Network Security Agency (INSA) are also monitoring online content to prevent online government criticism. Most prevalently, they use their control of telecom networks to filter the internet and block over 100 websites (Freedom House 2017b: 7). Through a combination of targeting Internet Protocol (IP) addresses and domains and deep-packet inspection, the state censors sites pertaining to opposition parties, human rights, diasporic dissent, and even the recent drought. It also blocks digital security tools like the anonymizing Tor browser, virtual private networks (VPNs), and the Electronic Frontier Foundation's guide to circumventing surveillance (Freedom House 2017b: 8).

As blogs and social media networks gain momentum in Ethiopia, officials are also increasingly monitoring and blocking these platforms' content. Bloggers who broach controversial topics often lose access to their sites and subsequently give up blogging. In the most notorious case, six bloggers from the Zone 9 Collective were even arrested and charged with terrorism for their online speech (Foltyn 2015). Facebook users who speak out online also receive threatening messages from anonymous accounts, or face phone calls and visits from security agents (Human Rights Watch 2014: 68). One user reported that he faced state harassment for posting an OLF flag on Facebook, while others stated that authorities forced them to change or remove their posts (Human Rights Watch 2014: 69).

When officials directly target their political opponents, they deploy an even more diverse array of surveillance techniques. However, the methods' level of technical sophistication depends on the gravity of the perceived threat and the power of the particular authority. At the lower end, local leaders, regional commanders, and federal police officers largely rely on rudimentary forms of surveillance. By contrast, the National Intelligence and Security Services (NISS), which oversees enforcement against terrorism and other domestic threats, conducts some of the most complex and formidable monitoring methods. Thus, even in a political and digital authoritarian regime, only certain organizations attain the fullest extent of authorization.

This hierarchy of power is evident in the differential forms of mobile phone surveillance wielded against activists. The most common method of lower-level and rural forces is to physically confiscate detained opponents' mobile devices. The officials then conduct warrantless searches of these detainees' contacts, messages, and phone logs to use that information in interrogations (Human Rights Watch 2014: 35). Meanwhile, higher-level authorities like the NISS have almost unrestricted access to the Ethio Telecom's comprehensive ZSmart database. This database, which Chinese company ZTE installed at the Ethiopian government's behest in 2009, can disclose phone records and other metadata. It can also reveal the contents of text messages and recorded conversations. According to former Ethio Telecom employees, intelligence agency officials can easily subject individuals to indefinite phone surveillance and themselves face no oversight (Human Rights Watch 2014: 39). As a method of intimidation, officials also present arrested activists and journalists with paper records or recordings of their phone calls during interrogation sessions (Human Rights Watch 2014: 42).

The Ethiopian government has also covertly adopted advanced surveillance technologies to target opponents outside of the country. In 2013, Citizen Lab security researchers discovered FinSpy, a remote monitoring system, on the computers of three members of the diaspora (Marquis-Boire et al. 2013). Among its capabilities, FinSpy can extract files from a computer's hard drive; enable live microphone and webcam surveillance; record communications taking place over email, chat, and Voice over Internet Protocol (VoIP); and monitor every feature of Skype (Finspy n.d.). Though FinSpy's maker, the British company Gamma Group, exclusively sells this tool to governments, observers have criticized its suspected sales to repressive states like Ethiopia, Turkmenistan, and Egypt (Higgins 2012). As Eva Galperin of the Electronic Frontier Foundation notes, "This is dual-use equipment. If you sell it to a country that obeys the rule of law, they

may use it for law enforcement. If you sell it to a country where the rule of law is not so strong, it will be used to monitor journalists and dissidents” (Perlroth 2012). In 2014, one U.S.-based target unsuccessfully sued Ethiopia, his native country, for allegedly infecting his computer with FinSpy and tracking his Skype calls, web searches, and website visits (Electronic Frontier Foundation 2017). These developments intimate that the EPRDR’s abusive practices extend beyond its national borders and reaffirm the dangers of the Ethiopian surveillance state’s increasingly unchecked power.

Conclusion

For a political and digital authoritarian regime like Ethiopia, the typical response to social unrest is to ramp up censorship and suppress freedoms. At the same time, the country’s desire for economic and technological expansion is dependent on raising rates of digital access and adoption. To reconcile this Authoritarian Dilemma, the EPRDF has strategically implemented some next-generation techniques of control. For instance, agencies have operationalized multiple scales and processes of surveillance to simultaneously expand and more flexibly delimit digital usage. While this shortsighted modulation of control may amplify governmental authority, it foments more distrust and resentment among the populace. Moreover, it ultimately weakens the prospects of national development. The overt and opaque manifestations of state surveillance chill the potentialities of free expression and dissent, and constrain many of the productive and creative ways that Ethiopians could newly engage with digital media channels. Controlling a vital new means of communications and critique also facilitates the acceleration of human rights violations, official opacity, and corruption. It fortifies authoritarian power at the expense of the tens of millions of people who must live under its suppressive state watch.

References

- Adejumobi, S.A. 2007. *The History of Ethiopia*. Westport, CT and London: Greenwood Press.
- Deibert, R. and Rohozinski, R. 2010. In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA and London: The MIT Press.
- Donovan, K.P. and Martin, A.K. 2014. “The rise of African SIM registration: The emerging dynamics of regulatory change.” *First Monday* 19 (2-3). Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820>.
- Economist Intelligence Unit. 2017. “Democracy Index 2016.” Accessed April 22, 2017. Available at: http://www.eiu.com/public/topical_report.aspx?campaignid=DemocracyIndex2016.
- Electronic Frontier Foundation. Last updated 2017. “Kidane v. Ethiopia.” Accessed April 22, 2017. Available at: <https://www EFF.org/cases/kidane-v-ethiopia>.
- Erixon, F. and Lee-Makiyama, H. 2011. “Digital Authoritarianism: Human Rights, Geopolitics and Commerce.” *ECIPE Occasional Paper* 5: 1-23.
- Federal Democratic Republic of Ethiopia. 2016. “Growth and Transformation Plan II (GTP II) (2015/6-2019-20).” Accessed April 22, 2017. Available at http://dagethiopia.org/new/images/DAG_DOCS/GTP2_English_Translation_Final_June_21_2016.pdf.
- Freedom House. 2007. “Freedom in the World: Ethiopia Report 2006.” Accessed April 22, 2017. Available at: <https://freedomhouse.org/report/freedom-world/2006/ethiopia>.
- FinSpy. n.d. “Remote Monitoring & Infection Solutions.” Accessed April 22, 2017. Available at: https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf.
- Foltyn, S. 2015. “Ethiopian bloggers on trial in case seen as crackdown on free expression.” *Washington Post*. Accessed April 22, 2017. Available at: https://www.washingtonpost.com/world/africa/ethiopian-bloggers-on-trial-in-case-seen-as-crackdown-on-free-expression/2015/04/20/d6813d84-d188-11e4-8b1e-274d670aa9c9_story.html.
- Freedom House. 2008. “Freedom in the World: Ethiopia Report 2007.” Accessed April 22, 2017. Available at: <https://freedomhouse.org/report/freedom-world/2007/ethiopia>.
- Freedom House. 2017a. “Freedom in the World: Ethiopia Report 2016.” Accessed April 22, 2017. Available at: <https://freedomhouse.org/report/freedom-world/2016/ethiopia>.
- Freedom House. 2017b. “Freedom on the Net 2016: Ethiopia.” Accessed April 22, 2017. Available at: <https://freedomhouse.org/sites/default/files/FOTN%202016%20Ethiopia.pdf>.
- Higgins, P. 2012. “Elusive FinFisher Spyware Identified and Analyzed.” *Electronic Frontier Foundation*. Accessed April 22, 2017. Available at: <https://www EFF.org/deeplinks/2012/07/elusive-finfisher-spyware-identified-and-analyzed>.
- Human Rights Watch. 2014. ““They Know Everything We Do”: Telecom and Internet Surveillance in Ethiopia.” Available at: https://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf.

- International Telecommunication Unit. 2016. "Percentage of individuals using the Internet, 2000-2015." Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/Individuals_Internet_2000-2015.xls.
- Kedzie, C. 1997. "Communication and Democracy: Coincident Revolutions and the Emergent Dictators." PhD dissertation. Accessed April 22, 2017. Available at: https://web.archive.org/web/20161221195757/http://www.rand.org/pubs/rgs_dissertations/RGSD127/sec2.html.
- Kerr, J. 2014. "The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States." Stanford University Social Science Seminar Series paper. Accessed April 22, 2017. Available at: http://cisac.fsi.stanford.edu/sites/default/files/kerr_-_cisac_seminar_-_oct_2014_-_digital_dictators_dilemma.pdf.
- MacKinnon, R. 2011. "China's 'Networked Authoritarianism.'" *Journal of Democracy* 22(2): 32-46.
- Marquis-Boire, M., Marczak, B., Guarnieri, C. and Scott-Railton, J. 2013. "You Only Click Twice: FinFisher's Global Proliferation." Citizen Lab Research Brief 15. Accessed April 22, 2017. Available at: <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2>.
- Nyst, C. 2012. "With new promise comes new perils: ICTs and the right to privacy in Africa." *Privacy International*. Accessed April 22, 2017. Available at: <https://www.privacyinternational.org/node/404>.
- Perlroth, N. 2012. "Software Meant to Fight Crime Is Used to Spy on Dissidents." *New York Times*. Accessed April 22, 2017. Available at: <http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html>.
- Schemm, P. 2016. "Dozens killed in Ethiopia after police use tear gas on protesters at festival." *Washington Post*. Accessed April 22, 2017. Available at: https://www.washingtonpost.com/world/africa/dozens-killed-in-ethiopia-after-police-tear-gas-protest-at-festival/2016/10/02/6e1d8f50-88b0-11e6-875e-2c1bfe943b66_story.html.
- Schemm, P. 2017. "Despite outward calm, Ethiopia extends state of emergency." *Washington Post*. Accessed April 22, 2017. Available at: https://www.washingtonpost.com/world/despite-outward-calm-ethiopia-extends-state-of-emergency/2017/03/30/b5544098-1529-11e7-ada0-1489b735b3a3_story.html.
- Saleh, N. 2012. "Egypt's digital activism and the Dictator's Dilemma: An evaluation." *Telecommunications Policy* 36(6): 476-483.
- Shaban, A.R.A. 2016. "Ethiopia partially lifts internet shutdown amid protest tension." *Africa News*. Accessed April 22, 2017. Available at: <http://www.africanews.com/2016/10/05/ethiopia-partially-lifts-internet-shutdown-amid-protest-tension/>.
- Solomon, T. 2014. "Ethiopia: Ericsson snatches more than half of China's ZTE telecom deal." *Africa Report*. Accessed April 22, 2017. Available at: <http://www.theafricareport.com/East-Horn-Africa/ethiopia-ericsson-snatches-more-than-half-of-chinas-zte-telecom-deal.html>.
- Toggia, P. 2012. "The revolutionary endgame of political power: the genealogy of 'red terror' in Ethiopia." *African Identities* 10(3): 265-280. Accessed April 22, 2017. Available at: <http://www.tandfonline.com/doi/abs/10.1080/14725843.2012.715455>.
- Winsor, M. 2015. "Ethiopia Elections 2015: Ruling Party Declares Historic 100 Percent Victory In Parliamentary Polls." *International Business Times*. Accessed April 22, 2017. Available at: <http://www.ibtimes.com/ethiopia-elections-2015-ruling-party-declares-historic-100-percent-victory-1979220>.
- World Bank. n.d. "Rural population (% of total population)." Accessed April 22, 2017. Available at: <http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS>.