Immigration and Refugee Board of Canada

Responses to Information Requests

Responses to Information Requests (RIR) respond to focused Requests for Information that are submitted to the Research Directorate in the course of the refugee protection determination process. The database contains a seven-year archive of English and French RIRs. Earlier RIRs may be found on the UNHCR's Refworld website. Please note that some RIRs have attachments which are not electronically accessible. To obtain a PDF copy of an RIR attachment, please email the Knowledge and Information Management Unit.

2 February 2017

ETH105729.E

Ethiopia: Information on the ability of the Ethiopian government to monitor and censor Ethiopian dissidents living in Canada, including scope and type of surveillance, and technology used; treatment of returning dissidents from Canada, including whether particular profiles face greater risks upon return (2014-January 2017)
Research Directorate, Immigration and Refugee Board of Canada, Ottawa

Information on the monitoring of dissidents living in Canada could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

1. Ability of the Ethiopian government to monitor and censor Ethiopian dissidents
1.1. Monitoring of dissidents

According to Human Rights Watch's *World Report 2016: Events of 2015*, the Ethiopian government "regularly monitors and records telephone calls of family members and friends of suspected opposition members and intercepts digital communications with highly intrusive spyware" (Human Rights Watch 27 Jan. 2016). The US Department of State's *Country Reports on Human Rights Practices 2015* similarly states that "authorities monitored telephone calls, text messages, and emails" (US 13 Apr. 2016). In correspondence sent to the Research Directorate, a senior researcher on the Horn of Africa with Human Rights Watch Human Rights Watch further indicated that Ethiopian authorities also monitor dissidents in the Ethiopian diaspora (Human Rights Watch 27 Jan. 2017).

The same source stated that Ethiopian authorities "have informants who attend public events" to monitor dissidents living outside of Ethiopia, as well as "individuals who monitor public social media posts," although "[a] lot of this is just for intel[ligence] gathering" (Human Rights Watch 27 Jan. 2017). The same source explained that there are "[v]arying opinions on how high a profile you need to be in order to be monitored in this way. High profile individuals definitely are, but sometimes individuals who wouldn't seem to be of much interest are also monitored" (Human Rights Watch 27 Jan. 2017).

A March 2014 Human Rights Watch report on telecom and internet surveillance methods used by Ethiopian authorities cites "former [government] officials" as indicating that they were involved in gathering intelligence on Ethiopians living in the diaspora, which

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. (Human Rights Watch March 2014, 18)

The same source adds that

[t]here 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. (Human Rights Watch March 2014, 18)

Corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

1.2 Electronic surveillance

Freedom House's *Freedom on the Net 2016* indicates that "exiled dissidents have been targeted by surveillance malware" (Freedom House 2016b). Similarly, according to a February 2014 *Washington Post* article, there are cases which have given rise to suspicion that the government of Ethiopia "has used sophisticated Internet technology to monitor its perceived enemies, even when they are in other countries;" the source cites a staff attorney for the Electronic Frontier Foundation, a "civil liberties group based in San Francisco," as stating that "[t]he Ethiopian government appears to be doing everything it can to spy on members of the diaspora, especially those in contact with opposition groups" (*The Washington Post* 18 Feb. 2014). The Human Rights Watch Senior Researcher also noted that government authorities have used malware to monitor the activities on the computers of the "highest profile targets in the diaspora" (Human Rights Watch 27 Jan. 2017). According to the same source, "[m]ost of the corroborated cases of infected computers come from those allegedly connected to [opposition group] Ginbot 7 (Human Rights Watch 27 Jan. 2017).

In a February 2014 report, Citizen Lab [1] describes three attempts within two hours on 20 December 2013 to install spyware "designed to steal files and passwords, and intercept Skype calls and instant messages" on computers of two ESAT [Ethiopian Satellite Television] [2] employees, one based in the US and one based in Belgium (Citizen Lab 12 Feb. 2014). An article on Mashable, "a global, multi-platform media and entertainment company" website with "tech, digital culture and entertainment content" (Mashable n.d.), cites a researcher of the Citizen Lab involved in writing the report as stating that he believed the Ethiopian government to be behind these attempts (Mashable 12 Feb. 2014). The same source cites another researcher involved in writing the Citizen Lab report as saying that "this type of targeted surveillance is a common method for tracking [diaspora journalists]" (Mashable 12 Feb. 2014). Corroborating information could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

A February 2014 article from Voice of America (VOA) reports that an Ethiopian refugee in London, who "identified himself as a member of the executive committee" of Ginbot 7, asked police to investigate evidence that his computer was hacked (VOA 20 Feb. 2014). According to its website, Privacy International, "a London-based anti-surveillance advocacy group" (Fusion 4 June 2015), filed a criminal complaint on behalf of this refugee to the UK's National Cyber Crime Unit of the National Crime Agency in February 2014, asking it to investigate "the potentially unlawful interception of communications [from the Ethiopian refugee] as well as the role a British company played in developing and exporting the invasive commercial surveillance software" (Privacy International 20 Feb. 2014). Information on the results of the complaint could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

A March 2015 Citizen Lab report describes further attempts to hack computers of ESAT employees with spyware on 5 and 10 November, and 9 December 2014, carried out by "the same governmental attacker" who was involved in the December 2013 attack (Citizen Lab 9 March 2015). According to Freedom House, the software used in this case "is advertised as 'offensive technology' sold exclusively to law enforcement and intelligence agencies around the world, [which] has the ability to steal files and passwords and intercept Skype calls and chats" (Freedom House 2016b). Similarly, Freedom House reported that leaked emails indicated that the Ethiopian government was paying the Italian company that supplies this software as late as March 2015 (Freedom House 2016a). An article on Motherboard, a subsection of the VICE website, cites an ESAT journalist targeted in the hacking attempt as stating that the Ethiopian authorities were "probably most interested" in his data and contacts; "they want to persecute the people that speak to ESAT" (Motherboard 9 Mar. 2015).

1.3 Censorship

Human Rights Watch's *World Report 2017* states that

the government regularly restricts access to social media apps and some websites with content that challenges the government's narrative on key issues. During particularly sensitive times, … the government blocked access to the internet. The government also jammed the signals of international radio stations like Deutsche Welle and [VOA] in August and September. (Human Rights Watch 17 Jan. 2017)

The same source adds that, under a state of emergency imposed in 2016, "people [in Ethiopia were] banned from watching diaspora television" (Human Rights Watch 17 Jan. 2017). Similarly, according to Freedom

House, "Ethiopia has a nationwide, politically motivated internet blocking and filtering regime that is reinforced during sensitive political events" (Freedom House 2016b). According to the US State Department's *Country Reports 2015*,

[t]he government periodically restricted access to certain content on the internet and blocked several websites, including blogs, opposition websites, and websites of Ginbot 7, the OLF [Oromo Liberation Front], and the ONLF [Ogaden National Liberation Front]. The government also temporarily blocked news sites such as al-Jazeera and the BBC. Several news blogs and websites run by opposition diaspora groups were not accessible. These included Addis Neger, Nazret, Ethiopian Review, CyberEthiopia, Quatero Amharic Magazine, Tensae Ethiopia, and the Ethiopian Media Forum. Authorities took steps to block access to Virtual Private Network providers that let users circumvent government screening of internet browsing and email. (US 13 Apr. 2016, 14-15)

Freedom House adds that during the anti-government Oromia protests that started in November 2015, more websites were "newly blocked," including "the websites of US-based diaspora satellite television stations such as [ESAT] and the Oromo Media Network (OMN)," as well as Ayyantuu.net and Opride.com, "prominent websites known for their reporting on the protests" (Freedom House 2016b).

Without providing further details, the Human Rights Watch Senior Researcher stated that

[s]elf-censorship is definitely increasing. It partially depends on which ethnic community individuals are from, but many high profile individuals in the diaspora have their family targeted back home. There isn't a lot documented on this in part [because] individuals in the diaspora do not want the reprisals publicized [because] of the perception it could make things worse for their targeted families. The threat of reprisals causes some to self-censor their activities in the diaspora, including what they say in public or post on social media. Reprisals against family members seem to be particularly prevalent in the Somali and Amhara communities. (Human Rights Watch 27 Jan. 2017)

2. Treatment of Returning Dissidents

Information on the treatment of returning dissidents in Ethiopia was scarce among the sources consulted by the Research Directorate within the time constraints of this Response.

In its English-language summary of an April 2015 Norwegian-language report on the situation of returnees who have been politically active in exile, Landinfo, the Norwegian Country of Origin Information Centre, states the following:

There is limited specific information about what has happened with Ethiopians who have returned to Ethiopia. Therefore, it is very difficult to give reliable information about what will happen with Ethiopians in exile who may be returned to Ethiopia by force and who are critical to the Ethiopian regime. Landinfo has experienced that the sources are vague and cautious in its [sic] statements about what may happen when Ethiopians are returned. The sources we have met differ on what may happen. Landinfo's assessment is that those who will be under the Ethiopian authorities' suspicion are, first and foremost, people they apprehend as a threat and who may mobilize and are prepared to use military force for change. (Norway 28 Apr. 2015, 3)

The Human Rights Watch Senior Researcher stated that, both in the case of dissidents who return home to visit or failed asylum claimants who are sent back to Ethiopia, "individuals who are known dissidents are at high risk of detention. Mistreatment and torture in detention are common" (Human Rights Watch 27 Jan. 2017). The same source added, without providing further detail, that "higher profile individuals are sometimes treated better" (Human Rights Watch 27 Jan. 2017).

Information on treatment of dissidents returning to Ethiopia from Canada could not be found among the sources consulted by the Research Directorate within the time constraints of this Response.

This Response was prepared after researching publicly accessible information currently available to the Research Directorate within time constraints. This Response is not, and does not purport to be, conclusive as to the merit of any particular claim for refugee protection. Please find below the list of sources consulted in researching this Information Request.

Notes

[1] The Citizen Lab is "an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto," which focuses on "advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security" (Citizen Lab, n.d.). According to their website, the Citizen Lab undertakes "research that monitors, analyses, and impacts the exercise of power in cyberspace" (Citizen Lab, n.d.).

[2] ESAT is "an independent satellite television station, radio and online news media outlet run by members of the Ethiopian diaspora" (Citizen Lab 12 Feb. 2014).

References

Citizen Lab. 9 March 2015. Bill Marczak, John Scott-Railton, Sarah McKune. "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware." [Accessed 23 Jan. 2017]

Citizen Lab. 12 February 2014. Bill Marczak, Claudio Guarnieri, John Scott-Railton, Morgan Marquis-Boire. "Hacking Team and the Targeting of Ethiopian Journalists." [Accessed 1 Feb. 2017]

Citizen Lab. N.d. "About the Citizen Lab." [Accessed 1 Feb. 2017]

Freedom House. 2016a. "Ethiopia." *Freedom in the World 2016*. [Accessed 23 Jan. 2017]

Freedom House. 2016b. "Ethiopia." *Freedom on the Net 2016*. [Accessed 23 Jan. 2017]

Fusion. 4 June 2015. Daniel Rivero. "Meet The Privacy Activists Who Spy On The Surveillance Industry." [Accessed 23 Jan. 2017]

Human Rights Watch. 27 January 2017. Correspondence from a senior researcher to the Research Directorate.

Human Rights Watch. 17 January 2017. "Ethiopia." *World Report 2017: Events of 2016*. [Accessed 25 Jan. 2017]

Human Rights Watch. 27 January 2016. "Ethiopia." *World Report 2016: Events of 2015*. [Accessed 23 Jan. 2017]

Human Rights Watch. March 2014. *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia.* [Accessed 23 Jan. 2017]

Mashable. 12 February. 2014. Lorenzo Franceschi-Bicchierai. "Report: Ethiopian Government Hacks Journalists in U.S. and Europe." [Accessed 23 Jan. 2017]

Mashable. N.d. "About." [Accessed 1 Feb. 2017]

Motherboard. 9 March 2015. Lorenzo Franceschi-Bicchierai. "Ethiopia Allegedly Used Spyware Against US-Based Journalists (Again)." [Accessed 23 Jan. 2017]

Norway. 28 April 2015. Landinfo - Country of Origin Information Centre. *Temanotat Etiopia: Reaksjoner Ved Retur og Politisk Aktivitet I Eksil (Sur Place)*. [Accessed 23 Jan. 2017]

Privacy International. 20 February 2014. "Explained: Our Criminal Complaint on Behalf of Tadesse Kersmo." [Accessed 31 Jan. 2017]

United States (US). 13 April 2016. "Ethiopia." *Country Reports on Human Rights Practices for 2015*. [Accessed 23 Jan. 2017]

Voice of America (VOA). 20 February 2014. Peter Heinlein. "Ethiopia Accused of Using Spyware Against Citizens Living Abroad." [Accessed 23 Jan. 2017]

The Washington Post. Craig Timberg. "U.S. Citizen Sues Ethiopia for Allegedly Using Computer Spyware Against Him." [Accessed 23 Jan. 2017]

Additional Sources Consulted

Oral sources: Ethiopian Advocacy Association; Ethiopian Association of Edmonton; Ethiopian Association of Toronto; Lawyer and Human Rights Activist based in Toronto; Political Science Professor, California State University at San Bernardino; Unity for Human Rights Toronto.

Internet sites, including: Amnesty International; Austrian Centre for Country of Origin and Asylum Research and Documentation; Ayyantuu.net; BBC; Dutch Council of Refugees; ecoi.net; Ethiopar.net; Ethiopia – Embassy in Ottawa, Government Portal, Ministry of Foreign Affairs; Ethiopian Review; Ethiopian Satellite Television; Factiva; France – Office français de protection des réfugiés et apatrides; Germany – Federal Office for Migration and Asylum; International Cities of Refuge Network; Oromo Media Network; UK – Home Office; UN – Refworld.

Tips on how to use this search engine.

Top of Page

Date modified: 2016-01-05