GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

ETHIOPIA

The potential impact of digital surveillance on the uptake and use of the internet in Ethiopia

Ethiopian Free and Open Source Software Network (EFOSSNET)
Abebe Chekol
abechekol@yahoo.com

Introduction

Ethiopia is the oldest independent country in Africa and one of the oldest in the world.[1] Politically, Ethiopia is a federal republic under its 1994 constitution. The current ruling party, the Ethiopian People's Revolutionary Democratic Front (EPRDF), has governed Ethiopia since 1991. Since taking power, the EPRDF has led ambitious reform efforts to initiate a transition to a more democratic system of governance and decentralise authority. Although still considered one of the world's poorest countries, the second most populous nation in Africa has recorded fast growth over the last five years. In 2012/2013, its economy grew by 9.7%, which made it one Africa's top-performing economies.[2]

The latest survey from the World Economic Forum puts Ethiopia at 130th out of 148 countries in its Networked Readiness Index.[3] The index measures the ability of economies to leverage information and communications technologies (ICTs) to boost competitiveness and well-being. Internet usage in Ethiopia is still in its infancy, with less than 1.5% of Ethiopians connected to the internet and fewer than 27,000 broadband subscribers countrywide.

In the context of the International Principles on the Application of Human Rights to Communications Surveillance,[4] this report assesses the ICT development policy and legal environment in Ethiopia, and how digital surveillance could impact on this.

Policy and legal frameworks

Article 26 of the 1994 Ethiopian Constitution states with regard to the "Right to Privacy": "All persons have the right to the inviolability of their letters, post and communications by means of telephone, telecommunications and electronic devices." It further states: "Public officials shall respect and protect these rights. They shall not interfere with the exercise of these rights except in compelling circumstances and in accordance with specific laws which aim to safeguard national security, public safety, the prevention of crime, the protection of health, morals and the rights and freedoms of others."

There are, therefore, specific laws that allow public officials to interfere with the exercise of the rights of individuals granted in the constitution. These laws are as follows:

Anti-Terrorism Proclamation No. 652/2009.[5] Article 14 of the Anti-Terrorism Proclamation, on "Gathering Information", proclaims: "To prevent and control a terrorist act, the National Intelligence and Security Service may, upon getting a court warrant: a) intercept or conduct surveillance on the telephone, fax, radio, internet, electronic, postal and similar communications of a person suspected of terrorism; b) enter into any premise in secret to enforce the interception; or c) install or remove instruments."

Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013.[6] Under "Investigative Techniques", part 4 of Article 25 of this Proclamation declares: "For the purpose of obtaining evidence of money laundering or financing of terrorism or tracing proceeds of crime, the judicial organs may authorize crime investigation authorities, for a specific period, among others, to access computer systems, networks and servers; and to place [an individual] under surveillance or to intercept communication; and to intercept and seize correspondence."

Telecom Fraud Offence Proclamation No. 761/2012.[7] Under this law, evidence gathered through interception or surveillance in accordance with the Criminal Procedure Code and other rel-

1 www.ethioembassy.org.uk/fact%20file/a-z/history.htm

2 World Bank. (2012). *World Atlas*. www.worldatlas.com/aatlas/world.htm

3 Bilbao-Osorio, B., Dutta, S., & Lanvin, B. (Eds.) (2014). *The Global Information Technology Report 2014: Rewards and Risks of Big Data*. Geneva: World Economic Forum, INSEAD, and Johnson Graduate School of Management, Cornell University.

4 https://en.necessaryandproportionate.org/text

5 Federal Democratic Republic of Ethiopia. (2009). Anti-Terrorism Proclamation No. 652/2009.

6 Federal Democratic Republic of Ethiopia. (2013). Proclamation on Prevention and Suppression of Money Laundering and Financing of Terrorism, Proclamation No. 780/2013.

7 Federal Democratic Republic of Ethiopia. (2012). Telecom Fraud Offence Proclamation No. 761/2012.

evant laws will be admissible in court in relation to telecom fraud offences.

Key issues

There has been a proliferation of counter-terrorism legislation globally following 9/11, which is considered a turning point in the history of counter-terrorism.[8] As indicated above, Ethiopia also passed an anti-terrorism law in July 2009. Since its promulgation, this law and its application have been controversial. A recent BBC article[9] published on 25 March 2014, referring to a Human Rights Watch (HRW) report on Ethiopia, reported the Ethiopian government's use of imported technology (mainly from European and Chinese firms) to undertake surveillance on the phones and computers of its perceived opponents. The report points out that given that all phone and internet connections in Ethiopia are provided by a state-owned company, the government has the power to monitor communications and have access to all call records of all telephone users in the country. This includes access to recorded conversations that can be used in the interrogation of suspects. According to the HRW report, the government has extended its surveillance to Ethiopians living overseas. Ethiopians living abroad (mainly in the United Kingdom and the United States) have accused the government of using spy software on their computers.

In terms of the legality and legitimate aim of such action, the government has issued the anti-terrorism law on the grounds of the clear and present danger of terrorism in Ethiopia, coupled with the inadequacy of ordinary laws to deal with this reality. Furthermore, it also argues that the United Nations Security Council resolution 1373 (2001) requires countries (including Ethiopia) to pass the law.[10] However, given the fact that digital surveillance is a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, the proportionality of its application is feared to undermine the democratic process.

The Ethiopian Television and Radio Agency hosted a debate[11] in August 2013 among political parties on a range of issues relating to the Ethiopian anti-terrorism law and its application. While the incumbent ruling party argues the legitimacy of this law on the grounds of the clear and present danger of terrorism in Ethiopia, the opposition parties argued the impact of this law on democratic rights and processes in the country. Furthermore, this can be considered a means of popularising the law to create awareness among the wider public, given there is little evidence of the level of awareness among the public in general on the use and scope of digital surveillance techniques and powers stated in the law. There is also little awareness both among civil society and the legislature of international principles such as user notification, where individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, or the need for independent public oversight mechanisms.

With regard to the international principle on the integrity of communications and systems, where states should not compel service providers or hardware or software vendors to build surveillance or monitoring capability, the anti-terrorism law declares in Article 14 that "any communication service provider shall cooperate when requested by the National Intelligence and Security Service to conduct the interception."

A recent article in *Addis Fortune*[12] reflects concern for privacy and data protection amidst the growing use of the internet in Ethiopia and global digital intrusion. In this context, the international principle on safeguards for international cooperation suggests applying the higher level of protection for individuals where there are agreements between states. Furthermore, the international principle on safeguards against illegitimate access suggests that states should enact legislation criminalising illegal communications surveillance by public and private actors. In both instances, there is concern that Ethiopia does not have a legal framework that could make authorities liable for a breach of user data and cross-border cyber-security issues. This occurs in the context of a lack of concern from Ethiopian internet users on the subject, and is one important gap that needs to be addressed by the government. Such a gap is also noted in the Information and Communication Technology Policy of 2009, which clearly recognises the need, among other cyber-oriented laws, to issue a data protection law.

8 Kassa, W. D. (2013). Examining Some of the Raisons D'Être for the Ethiopian Anti-Terrorism Law. *Mizan Law Review*, 7(1).

9 BBC. (2014, March 25). Ethiopia uses foreign kit to spy on opponents – HRW. *BBC*. www.bbc.com/news/world-africa-26730437

10 United Nations Security Council Resolution 1373 (2001), adopted by the Security Council at its 4385th meeting, on 28 September 2001.

11 www.youtube.com/watch?v=-g5JhwpAt4U

12 Yilma, K. (2012, June 5). Unprepared Ethiopia faces privacy intrusion. *Addis Fortune*. addisfortune.net/columns/unprepared-ethiopia-faces-privacy-intrusion

As the number of internet users increases over time – the government plans to increase it to 3.69 million by the end of the Growth and Transformation Plan (GTP) period in 2015[13] – the data privacy of internet users in Ethiopia will undoubtedly become crucial if this sector is to contribute its share to the economy. A recent report from the McKinsey Global Institute[14] indicates that, as in many countries in Africa, the internet's contribution to Ethiopia's gross domestic product (GDP) is 0.6%, which is low compared to the leading countries of Senegal (3.3%) and Kenya (2.9%). Ethiopia falls under the category of countries that perform below their weight, along with Angola, Algeria and Nigeria.

It would therefore be important to assess the implications of digital surveillance on the growth of ICT-based services such as e-commerce[15] and e-government,[16] which are both key sectors given prominent attention in the implementation of the national ICT policy in Ethiopia. The Ministry of Communications and Information Technology is currently implementing the e-government strategy, which aims to develop more than 200 e-services (currently in different phases of implementation) and get 20% of government departments online.[17] There is also evidence of the growing use of ICTs in business, with internet use in companies in Ethiopia rated at 3.6 on a 0 to 7 index range.[18] It is therefore important to review the impact of laws on the growth and use of the internet in various sectors.

For example, although the proclamation on the "Prevention and Suppression of Money Laundering and Financing Terrorism" does not explicitly address e-commerce, there is a need to assess whether the provisions of the law have an impact on e-commerce broadly and electronic fund transfers specifically. Similarly, e-government could be affected by the legislation mentioned above in both positive and negative ways, which requires further investigation. While the intense focus on improving data collection and information practices and systems may contribute to the establishment of government-wide technical standards and best practices that could facilitate the implementation of new and existing e-government initiatives, it could also promote the use of secure web portals to help ensure the data integrity of transactions between the government and citizens and business. However, concerns about the potential abuses of data collection provisions could jeopardise citizen enthusiasm for carrying out electronic transactions with the government.

With the evolution of the internet and digital communications, new trends are emerging and regulatory interventions are becoming even more complex in the context of these emerging issues – such as the revelations of widespread internet surveillance, human rights imperatives, the line between privacy versus security, and managing critical resources that make the internet possible. In this regard, governments should demonstrate greater transparency as regards their practices in the collection of personal data, taking into account the considerations of national security, citizen rights and public accountability.

Conclusions

The World Summit on the Information Society (WSIS) Action Plan recommends "cooperation among the governments at the United Nations and with all stakeholders as appropriate to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues." Though belated in realising the legal framework in changing circumstances, such as the growing ubiquity of the internet, the Ethiopian government has recently started working on these issues. Laws that regulate online behaviour and transactions are in the pipeline. A cyber-crime law, drafted by the Information Network Security Agency, and an e-commerce law, drafted by the Ministry of Communication and Information Technology in collaboration with the United Nations Economic Commission for Africa (UNECA), are examples. In this regard, the Conference of African Union Ministers of Justice adopted the African Union Convention on Cybersecurity and Personal Data Protection in May 2014. The Convention, which was drafted by UNECA in collaboration with the African Union Commission, and which has been reviewed through a series of sub-regional consultations with regional economic communities, is expected to be tabled before the African Union Heads of State and Government for ratification later this year. The Convention covers four areas, namely cyber security, combating cyber crime, electronic transactions (e-transactions), and

13 Ibid.

14 McKinsey & Company. (2013). *Lions go digital: The Internet's transformative potential in Africa*. Johannesburg: McKinsey Global Institute.

15 Commercial transactions on the internet, whether retail business-to-customer or business-to-business or business-to-government, are commonly called electronic commerce, or "e-commerce".

16 E-government involves using information technology, and especially the internet, to improve the delivery of government services to citizens, business, and other government agencies.

17 McKinsey & Company. (2013). Op. cit.

18 Ibid.

data protection and privacy. Countries will therefore be expected to amend their cyber security and data protection laws to bring them in line with the Convention.

This will help harmonise the existing legislation discussed above with respect to digital surveillance. While many of the provisions related to the surveillance and investigatory powers of law enforcement have raised concerns within the privacy and civil liberties communities, there is also the potential impact that this harmonisation can have on the growing use and application of ICTs in business through e-commerce, and government services through e-government. The challenge is to strike the balance on the use and application of these laws between the need for counter-terrorism measures and the imperative the respect to rights granted in the constitution.

Action steps

While close to 90 countries have so far issued data protection laws, Ethiopia has not. It is noted above that the Information and Communication Technology Policy of 2009, however, clearly recognises the need, among other cyber-oriented laws, to issue a data protection law.[19] Therefore there is a need for Ethiopia to develop a data protection and privacy law that can harmonise existing laws that affect these rights.

However, as much as establishing the requisite legal framework, raising public awareness about human rights and fundamental freedoms is very crucial. The Ethiopian Human Rights Commission is one stakeholder in this area in Ethiopia. It was established by law with the objective of "educating the public with the view to enhance its tradition of respect for and demand for the enforcement of human rights [through the public] acquiring sufficient awareness regarding human rights." The Commission needs to scale up its efforts in an era where the human right to privacy is being strongly challenged with the evolution of new and emerging technologies – and new state imperatives, such as countering terrorism.

The laws related to cyber crime and e-commerce need to be reviewed, not only to attune them to emerging challenges, but to address the challenges of data protection and privacy in order to build confidence and trust in the use of ICTs in general and the internet in particular.

19 Yilma, K. (2012, June 5). Op. cit.