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

KENYA

Is surveillance a panacea to Kenya's security threats?

Kenya ICT Action Network (KICTANet)
Victor Kapiyo and Grace Githaiga
www.kictanet.or.ke

Introduction

Kenya is located in East Africa and has an estimated population of over 43 million people.[1] The country has, according to recent estimates, 31.3 million mobile subscribers and 19.1 million internet users.[2]

Despite the country's relative peace, Kenya has since 1975 fallen victim to a number of sporadic terrorist attacks. And, since the 2011 Kenya Defence Forces (KDF) incursion in Somalia,[3] terrorist attacks in retaliation by groups such as Al Shabaab have increased, taking the form of grenade attacks or indiscriminate shooting, with the most recent incidents being the Westgate Mall siege,[4] the Gikomba grenade attack,[5] and the Mpeketoni massacre.[6] These incidents have raised public concern over Kenya's preparedness to combat terrorism.

In 2010, the country adopted a new constitution, which provides an expansive bill of rights, including, among others, privacy rights. However, the country still lacks dedicated privacy legislation following the state's repeated failure to adopt the Data Protection Bill 2013.[7] In 2012, parliament passed the much-criticised Prevention of Terrorism Act,[8] which provides the legal framework for counter-terrorism activities.

This report seeks to assess the implications of the government's response to terrorism through its proposal to introduce and adopt surveillance technology in major towns as a measure to avert future terror attacks.

Policy and political background

In its manifesto,[9] the Jubilee Government, elected in March 2013, proposed the use of CCTV cameras in fighting crime and a "buy Kenyan" procurement policy as solutions to Kenya's security problems. In this regard, in May 2014 it contracted Safaricom Limited[10] to build the Integrated Public Safety Communication and Surveillance System (IPSCSS) to help security forces fight crime.[11]

Opinion is divided – including in discussions on KICTANet[12] – on the appropriate ICT solutions to deal with the country's rising security problems. Some support the introduction of a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system, such as has been implemented in the US and Israel.[13]

However, some feel that technology alone is insufficient to counter terrorism.[14] They argue that the government should sort out the basics and invest in police reforms, attitude and behaviour change, police communication, police coordination and response to crime, anti-corruption measures, forensics, and effective prosecution of cases.

The project proposed by the Jubilee Government has been criticised as a continuation of the now well-established government approach of unsuccessfully throwing technology at problems without a corresponding re-organisation of bureau-

1 data.worldbank.org/country/kenya

2 The Kenya National ICT Masterplan 2013-2017, p. 16. https://www.kenet.or.ke/sites/default/files/Final%20ICT%20Masterplan%20Apr%202014.pdf

3 The Kenya Defence Forces incursion into Somalia sought to quell the Al Qaeda-linked Al Shabaab militant group under Operation "Linda Nchi" (Protect Country).

4 This occurred in September 2013, resulting in the death of 67 people and the wounding of 175 people. Westgate Shopping Mall attack. en.wikipedia.org/wiki/Westgate_shopping_mall_attack

5 May 2014, resulting in the death of 10 people and the wounding of 70 people. Samwel, O. (2014, May 17). 10 killed and 71 injured in Gikomba terror attack. *The People*. www.mediamaxnetwork.co.ke/thepeople/76951/ten-killed-71-injured-gikomba-terror-attack

6 June 2014, resulting in the death of 60 people. Ongiri, I., & Namunane, B. (2014, June 17). Uhuru blames massacre on tribalism, hate politics. *Daily Nation*. www.nation.co.ke/news/Uhuru-blames-massacre-on-tribalism--hate-politics/-/1056/2352306/-/wyy1laz/-/index.html

7 www.cickenya.org/index.php/component/k2/item/download/299_b3de9506b20338b03674eacd497a6f3a

8 kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/PreventionofTerrorism_No30of2012_.doc

9 Jubilee Coalition. (2013). *Transforming Kenya: Securing Kenya's Prosperity, 2013-2017*. issuu.com/jubileemanifesto/docs/jubilee_manifesto/3

10 The leading mobile telecommunication network operator in Kenya. www.safaricom.co.ke

11 PSCU. (2014, May 14). Integrated communication, surveillance system to boost security. *Capital FM*.
www.capitalfm.co.ke/business/2014/05/integrated-communication-surveillance-system-to-boost-security

12 Online discussion on Security Situation in Kenya. www.kictanet.or.ke/?p=20030

13 Ibid., Gichuki John Chuksjonia via KICTANet.

14 Ibid., John Walubengo via KICTANet.

cratic procedures.[15] Similar projects include the primary school laptop project, so-called "digital speed governors",[16] cashless payment for public transport, speeding cameras, biometric voter registration, electronic voting, and the electronic transmission of election results.

The proposed surveillance project

The IPSCSS[17] will result in the installation of 1,800 CCTV cameras with face and motor vehicle number plate recognition capabilities in strategic locations in Kenya's two big cities of Mombasa and Nairobi; setting up a command and control centre where footage from the CCTV cameras and handheld devices will be relayed in real time; a video conferencing system connecting 195 police stations; with high-speed internet; the development of a 4G LTE[18] network for the police with 80 base stations; supplying the police with 7,600 radio communication devices with SIM cards and photo and video capability; and linking 600 police vehicles to the command and control centre.

The goal of the project is to, among other things, enable security agents to communicate better and boost their capacity to fight terrorism.[19] The government has also put in place a National Cyber Security Strategy[20] to counter the ever-evolving cyber threats.

Safaricom Limited was single-sourced to develop the project, expected to cost 14.9 billion shillings (USD 169.6 million),[21] which will go up to 18.8 billion shillings (USD 214 million) after taxes.[22] Safaricom is expected to provide maintenance and support over a five-year period at a cost of 440 million shillings (USD 5 million) annually.[23]

The project has caused a lot of controversy. It has emerged that it is similar to a previous controversial tender, which was cancelled, pitting Chinese firms Huawei and ZTE against each other. These firms are currently embroiled in litigation over the issue.[24] Further, the decision to single-source the tender and award it to the mobile provider Safaricom has resulted in the suspension of the project by the Kenyan National Assembly's Committee on Administration and National Security. This is due to queries over the project cost, the choice of Safaricom as the supplier, its technical capacity, and its foreign ownership. Other queries relate to the opaqueness of the procurement and possible violation of procurement law, corruption allegations, and the secrecy, speed and purported urgency of the procurement.[25]

Implications of the proposed surveillance project

This section focuses on the implications of the proposed surveillance project, and, more particularly, the impact that the use of CCTV with facial recognition technology has on privacy rights guaranteed in the Constitution of Kenya.

Facial recognition technology enables the identification or authentication of individuals by comparing their face against a database of known faces and searching for a match.[26] The process requires a computer to find a face in the image, and then create a numeric representation of the face based on the relative position, size and shape of facial features. Thereafter, the numeric "map" of the face in the image is compared to a database of images of faces, such as a national identification database.

15 Walubengo, J. (2014, June 17). Without changes to policing, Safaricom's cameras may struggle to deliver. *Daily Nation*. www.nation.co.ke/oped/blogs/dot9/walubengo/-/2274560/2351214/-/11w8ih4z/-/index.html

16 Gerald Andae, G. (2014, January 1). Agency orders matatus to install new speed governors. *Business Daily Africa*. 1 January 2014, accessed 19 July 14, www.businessdailyafrica.com/Agency-orders-matatus-to-install-new-speed-governors/-/539546/2131568/-/ccfie9/-/index.html

17 The National Police Integrated Public Safety Communication and Surveillance Project; see also: Wokabi, C. (2014, June 14). Safaricom to face MPs over Sh15bn security contract. *Daily Nation*. www.nation.co.ke/news/Safaricom-to-face-MPs-over-Sh15bn-security-contract/-/1056/2349044/-/mx7va5/-/index.html

18 https://sites.google.com/site/lteencyclopedia/home

19 Daily Nation. (2014, May 13). Why State House made a call to Safaricom chief over insecurity. *Daily Nation*. www.nation.co.ke/news/Why-State-House-made-a-call-to-Safaricom-chief-over-insecurity/-/1056/2313756/-/ybd3dt/-/index.html

20 www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf

21 Calculated at a rate of 87.94 Kenyan shillings (KES) per 1 USD.

22 Ngirachu, J. (2014, July 1). Safaricom security tender to be audited, says Rotich. *Daily Nation*. www.nation.co.ke/business/Safaricom-security-tender-to-be-audited-says-Henry-Rotich/-/996/2368428/-/wy2sp2/-/index.html

23 Kiplangat, J. (2014, June 18). Safaricom to be paid Sh440m every year. *Daily Nation*. www.nation.co.ke/news/Safaricom-to-be-paid-Sh440m-every-year-/-/1056/2353672/-/b1ff14z/-/index.html

24 Wokabi, C. (2014, May 13). Sh14bn Safaricom deal to boost war on terror. *Daily Nation*. www.nation.co.ke/news/Sh14bn-Safaricom-deal-to-boost-war-on-terror/-/1056/2313684/-/afydehz/-/index.html; see also: Teyie, A. (2014, July 5). Intrigues of lucrative government tenders. *Daily Nation*. mobile.nation.co.ke/news/Intrigues-of-lucrative-government-tenders/-/1950946/2373320/-/format/xhtml/-/sgsya3/-/index.html

25 Wafula, C. (2014, June 5). Safaricom security deal placed on hold. *Daily Nation*. www.nation.co.ke/news/politics/Safaricom-security-deal-placed-on-hold-/-/1064/2338948/-/eqcohoz/-/index.html; Ngirachu, J. (2014, June 4). Three MPs question Safaricom security deal. *Daily Nation*. www.nation.co.ke/news/politics/Three-MPs-question-Safaricom-security-deal/-/1064/2336670/-/2t3x1vz/-/index.html

26 Office of the Privacy Commissioner of Canada. (2013). *Automated Facial Recognition in the Public and Private Sectors*. www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.asp

The use of such technologies is on the increase, and there is now widespread use and application in law enforcement, border control, the military, casinos, on mobile phones, and on social media sites such as Facebook. However, there are still concerns over the introduction of CCTV cameras with facial recognition capacity in fighting crime in Kenya.

Article 31 of the Constitution of Kenya provides for the right to privacy, which includes the right for a person not to have their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily acquired or revealed; or the privacy of their communications infringed on. Further, Article 24 provides for the limitation by law of a right or fundamental freedom, but only to the extent that it is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.[27]

Section 35 of the Prevention of Terrorism Act limits the constitutional right to privacy, but only for purposes of investigating acts of terrorism; the detection and prevention of a terrorist act; and ensuring that the enjoyment of rights and fundamental freedoms by an individual does not prejudice the rights and fundamental freedom of others.

The proposed Data Protection Bill, 2013, does not recognise images or video recordings of an individual as personal data. However, the bill reinforces the right to privacy and provides best practices and principles in data protection compliance, and regulates the collection, retrieval, processing, storage, use and disclosure of personal data. In these circumstances, the introduction and use of facial recognition technology in the absence of clear regulation means there is hardly any protection from the abuse of collected images.

The government has maintained that the legitimate aim of the project is to enable law enforcement to identify terrorists. However, this goal presupposes the knowledge of the identity of the terrorists, which is debatable. As a result, the use of the technology opens the system up for abuse and application in a manner that is discriminatory. Even before the introduction of CCTVs, Kenyan police conducted raids targeting persons of either Somali heritage, Muslim faith or both. The unregulated use of CCTV cameras will only catalyse such profiling.

While the use of facial recognition technology has its benefits, its unregulated use may infringe upon human rights. It has been reported that the government does not have a database of photos to use to compare their results with, as the current photos on IDs are unintelligible to computers.[28] As such, without such a database, it is not meaningful to implement such a system, especially in light of the other security needs and priorities.

The use of facial recognition technology will allow the identification of any person by name and in secret from a photo taken on the street, from the internet or other sources such as social media sites like Facebook. In addition, it will allow the police to capture images *en masse*, and maintain a photo and video database of the political and non-criminal activities of anyone. This poses threats to freedom of expression and association. Moreover, there is no limitation on the scale of surveillance that the CCTV system will cover.

The use of the technology also poses challenges to due process, as neither judicial authorisation nor the consent of the individual is required for the surveillance, opening up the system to illegitimate access. This means that law enforcement, in the absence of clear guidelines and safeguards, can abuse the system, and without any legitimate reason or cause, covertly use facial recognition on anyone without their permission, without any meaningful transparency or accountability, and for unjustified purposes for which the system was not originally intended.

Additionally, the technology will allow the state to tap into the existing databases and use facial recognition to identify people using their national identification records or the Independent Electoral and Boundaries Commission biometric voter register.

It should be noted that there is no independent public oversight body to regulate how the information collected will be managed. While the Independent Policing Oversight Authority[29] has been established, it has a limited mandate that focuses on investigation of complaints related to disciplinary or criminal offences committed by members of the National Police Service, and can only make recommendations based on its findings. Further, while the Data Protection Bill proposes to confer to the Commission on Administrative Justice the mandate and responsibility to enforce its provisions, the bill is yet to be passed and the Commission cannot therefore assume such functions.

27 The relevant factors include, among others: the nature of the right, purpose and extent of limitation; the existence of less restrictive means to achieve the purpose; and the need to ensure the enjoyment of rights does not prejudice the rights of others.

28 Odongo, W. (2014, June 8). Cameras will not save us. *Daily Nation*. www.nation.co.ke/lifestyle/Cameras-will-not-save-us/-/1190/2341040/-/b7i90pz/-/index.html

29 ipoa.go.ke/index.php/functions-of-authority

Lastly, the fact that Safaricom, which is Kenya's largest telecommunications service provider, is building the system raises doubt about the integrity of the system, the company's independence, and the apparent conflict of interest. The company has over 20 million subscribers[30] whose personal information it keeps pursuant to laws requiring SIM card registration. There are fears that its role in the development of the system may compromise its independence, including that of its network. There are also worries that Safaricom will enable law enforcement to easily access its database of users to match with the facial recognition data. The company in recent times came under sharp criticism for disclosing personal information to third parties as part of its bulk SMS services, despite clear provisions to the contrary in its terms and conditions.[31]

Conclusions

It is important to note that despite the presence of constitutional guarantees on the right to privacy, the absence of a proper policy and legislative regime for privacy protection means that the use of facial recognition technology in surveillance will result in serious implications for privacy and personal safety and lead to the violation of fundamental rights and freedoms. Therefore, it is time for laws that limit the use of facial recognition data collection.

A report[32] by the US National Academy of Sciences has concluded that biometric recognition technologies are inherently probabilistic and fallible. In addition, according to the Surveillance Studies Centre at Queen's University in Ontario, Canada, urban surveillance systems have not been proven to have any effect on deterring criminals.[33]

Whereas fears over insecurity have led to different sectors of society welcoming the introduction of the project, it must be stated that technology alone is insufficient to deal with crime. It can only be used to complement other initiatives by law enforcement to fight crime. Facial recognition technologies are not always foolproof or accurate. And as such, they ought to be designed and implemented with not only this in mind, but also with consideration to the social, legal and cultural factors that can affect the effectiveness and acceptance of the systems.

Action steps

Moving forward, the following are recommended:

- The Data Protection Bill 2013 should be amended to take cognisance of facial recognition technologies, and its adoption fast-tracked.
- There is a need for clear regulations and safeguards on the collection, access, retrieval, processing, storage, use and disclosure of personal data, including biometric information. This includes legislation that governs intermediaries.
- The proposed surveillance project should not start before the adoption of proper privacy safeguards, including the Data Protection Bill.
- A comprehensive privacy impact assessment should be conducted before developing and purchasing new technologies that will collect personal information including biometric data.
- The CCTV cameras should be located only in public spaces.
- Mechanisms should be put in place to regulate all state security, intelligence, policing, and other law enforcement agencies, to ensure they observe the rule of law and are transparent and democratically accountable.

30 About Safaricom, Safaricom, www.safaricom.co.ke/about-us/about-safaricom

31 Terms and Conditions, Safaricom. www.safaricom.co.ke/about-us/about-safaricom/terms-conditions

32 National Research Council. (2010). *Biometric Recognition: Challenges and Opportunities*. Washington, DC: The National Academies Press. https://download.nap.edu/login.php?record_id=12720&page=%2Fdownload.php%3Frecord_id%3D12720; see also: National Academy of Sciences. (2010, September 24). Automated biometric recognition technologies 'inherently fallible,' better science base needed. *The National Academies*. www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=12720

33 Kelly, H. (2013, April 26). After Boston: The pros and cons of surveillance cameras. *CNN.com*. edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings