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

CAMEROON

The stammerings of Cameroon's communications surveillance

PROTEGE QV
Sylvie Siyam and Serge Daho
www.protegeqv.org

Introduction

The Republic of Cameroon is a country in the west central Africa region. It is bordered by Nigeria, Chad, the Central African Republic, Equatorial Guinea, Gabon and the Republic of Congo.

In this country of nearly 21,700,000 people,[1] of which 1,006,494 are internet users[2] (representing roughly 5% of the population), according to the International Telecommunication Union (ITU), it is a real challenge to identify the presence of communications monitoring by the state. Nonetheless, we know that under the guise of national security and intelligence gathering, citizens' computers and internet communications are spied on by the government.

This was demonstrated when MTN's Twitter service in Cameroon was shut down on 8 March 2011. Wary about the role played by Twitter and other social networks in sparking an Egypt or Tunisia-style uprising, the government blocked MTN's Twitter service[3] for security reasons during what were later called "hunger riots" in our country.

Policy and political background

Since independence, Cameroon's successive constitutions have proclaimed its people's commitment to human rights as set out in the United Nations Universal Declaration of Human Rights and the African Charter on Human and Peoples' Rights. Our country is also party to major international and regional human rights conventions, including the International Covenant on Civil and Political Rights (ICCPR).

At the national level, the preamble to the constitution declares the Cameroonian people's commitment to the freedom of communication and expression.

Many laws and decrees dealing with freedom of communication and expression and with telecommunications and communications exist in Cameroon, some of which impact on surveillance:

- Law N° 98/014 of 14 July 1998, which regulates telecommunications.
- Law N° 2004/016 of 22 July 2004 creating the National Commission on Human Rights and Freedoms. The commission is an independent institution set up to promote and protect human rights in the country. Though important, none of its statutory provisions hint at the surveillance of communication.
- Law N° 2010/021 of 21 December 2010 governing electronic commerce.
- Law N° 2010/013 of 21 December 2010 governing electronic communications in Cameroon.
- Law N° 2010/012 of 21 December 2010 on cyber security and cyber crime. The latter "governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon." While this law was hailed by some as a much-needed step in the right direction to curb Cameroon's nascent or burgeoning cyber crimes industry, others have criticised it for being light on internet security and heavy on sanctions, particularly with regard to sanctioning online expression.
- Decree N° 2002/092/PR of 8 April 2002 creating the National Agency for Information and Communications Technologies (ANTIC). The ANTIC was created to facilitate and accelerate the uptake of ICTs in Cameroon so that they can contribute to the development of the country.
- Decree N° 2012/180/PR of 10 April 2012 assigning new missions to the ANTIC, including the regulation of electronic security activities and the regulation of the internet in Cameroon. With this decree, the ANTIC became the key actor in terms of restrictions imposed by the government on the free flow of online information.

1 countryeconomy.com/demography/population/cameroon

2 www.internetworldstasts.com. According to the World Bank, internet users are people with access to the worldwide network. This may include users who access the internet at least several times a week and those who access it only once within a period of several months.

3 MTN is a mobile telephone company that in March 2011 was the sole Twitter service provider in Cameroon.

- Decree N° 2013/0399/PM of 27 February 2013 establishing the modalities of protection for electronic communications consumers. This decree clearly states that when it comes to electronic services, the consumer is entitled to have his or her protection kept private.

"Weeding them out": Evidence of surveillance in Cameroon

There are few credible reports that the government monitors email or other internet- related activities in Cameroon. However, as certainly as everywhere throughout the world, Cameroon's administration does spy on citizens' emails to checkmate the activities of unscrupulous people capable of threatening its internal security. In 2009, the government launched a campaign aimed at capturing the personal information of mobile phone holders, allegedly "to ban the unfair use of the mobile phone [in a way that can prejudice] law and public order and ... citizens' safety."

The government's monopoly over all mobile and internet infrastructures through its sole, state-owned telecom operator, CAMTEL (Cameroon Telecommunications), facilitates communications surveillance. During an interview given to the online media outfit Cameroon-Info.Net,[4] Woungly Massaga, a Cameroonian dissident, stated his phones have always been tapped.

On 19 March 2014, the general manager of the ANTIC gave an interview to the government's daily newspaper *Cameroon Tribune* during which he further provided details on how social networks and websites are watched in Cameroon. To deal with ill-intentioned persons and the terrorist groups who use social networks to recruit followers and spread propaganda, he said, "The ANTIC uses state-of-the-art tools or cutting-edge tools to permanently watch social networks. This consists of browsing the various profiles on the social networks to detect illicit content representing a potential threat for the national security and the image of Cameroon, and to weed them out."[5]

When it comes to websites, the ANTIC uses a technical platform that scans web content using keywords to detect those inciting hatred, being slanderous, or representing a danger for the state. Though it is still unclear which technologies are used to monitor telecoms activity in Cameroon,[6] the interview shed light on the process that led to the shutting down of MTN's Twitter service in Cameroon from the 8 to the 18 March 2011 during peaceful protests. Prior to that, on 22 February 2011, Cameroonian government spokesperson Issa Tchiroma Bakary summoned journalists to his office for a media briefing in which he issued a warning directed at Cameroonians in the diaspora using social media tools such as Facebook and Twitter to call for a march to end the 29-year rule of President Paul Biya. The protest was to coincide with an opposition-led march in Douala to honour demonstrators killed by security forces during February 2008 anti-government protests.

A coalition of organisations led by Privacy International, Access and the Electronic Frontier Foundation has outlined a set of 13 International Principles on the Application of Human Rights to Communications Surveillance.[7] These include proportionality, competent judicial authority, due process and user notification. Did the blocking of MTN's Twitter[8] service meet these requirements?

At the time Twitter was blocked, only around 50 people[9] were affected by the suspension of MTN's service – so was it worth blocking it? This raises the proportionality principle: was there a high degree of probability that a serious crime was about to be committed by MTN's Twitter users?

The principles state: "Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent." Cameroon of course lacks a judicial mechanism to protect people from unlawful government surveillance. As a consequence, no judicial warrant was obtained to shut down MTN's service.

Another of the 13 Principles that was ignored by the government is the "due process" principle that requires states to respect and guarantee individuals' human rights by ensuring that lawful procedures surrounding communications surveillance are properly recorded and available to the general public. Cameroonian Minister of Communications and

4 Ngangué, Y. (2014, May 19). Interview de Woungly Massaga, Homme politique et nationaliste Camerounais: "Le Cameroun est une véritable bombe à retardement". *Cameroon-Info.Net*. www.cameroon-info.net/stories/0,61441,@,cameroun-20-mai-2014-interview-de-woungly-massaga-homme-politique-et-nationalist.html

5 Cameroon Tribune. (2014, March 29). [Interview] Cameroun: Dr Ebot Ebot Enow Directeur Général de l'Agence Nationale des TIC. *Afro Concept News*. www.afroconceptnews.com/2014/03/29/interview-cameroun-dr-ebot-ebot-enow-directeur-general-de-lagence-nationale-des-tic

6 It is worth pointing out that the Chinese telecom giants ZTE and Huawei, major players in the African and global telecom industry, are CAMTEL's telecom equipment suppliers in Cameroon.

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

8 The Twitter via SMS service offered by MTN Cameroon, one of three telecommunications operators in the country, allowed anyone with a regular phone to punch in a code and start receiving tweets for free.

9 The deal between MTN Cameroon and Twitter was concluded on December 2010 when the smartphone adoption and internet penetration rates were relatively low in Cameroon.

government spokesman Issa Tchiroma told Agence France Presse that "it was the government's job to protect the nation," and that the Twitter service was blocked "for the highest interest of the state." While this may be true, Cameroon is party to the International Covenant on Civil and Political Rights (ICCPR), and Article 19 of the ICCPR guarantees the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers." Article 9 of the African Charter on Human and Peoples' Rights, to which our country is also party, guarantees that every individual shall have the "right to receive information" and "to express and disseminate his opinions within the law." The government's job is not only "to protect" the nation, but also to protect and guarantee its citizens' rights, and one of the most fundamental of these is the right to communicate – the internet has become a key means by which individuals can exercise their right to freedom of opinion and expression.[10]

Concerning the "user notification" principle, individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision. An 8 March 2011 tweet by Bouba Kaele, marketing manager of the Cameroon division of MTN, announced that "[f]or security reasons, the government of Cameroon requests the suspension of the Twitter SMS integration on the network." MTN later confirmed the suspension without explanation: "Twitter SMS Connectivity Service suspended from March 07, 2011 till further notice." As a result, Twitter users were not informed prior to the service shutdown and the suspension caught them by surprise. The shutdown prompted an outcry from Reporters Without Borders, which condemned the lack of transparency surrounding the block and feared its implications for online freedom of expression in Cameroon. They said: "We hope the blocking of Twitter via SMS is not a prelude to other kinds of censorship of mobile phone services or tighter controls on the internet. Everything suggests that the authorities are trying to stop microblogging. We deplore the apparent readiness to impose censorship for the least reason, especially when the target is the peaceful expression of opinions."[11]

Conclusion

Nearly every country in the world recognises the right to privacy explicitly in its constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Though it exists, communications surveillance, as far as we know, is not pervasive in Cameroon. Nevertheless, from our story, we learned that the government decision did not take into account people's legitimate and fundamental right to freely seek and receive information or to communicate. Most agree that national security[12] and the fight against terrorism might justify restrictions on the free flow of online information. However, these restrictions must be founded upon evidence that there is a high degree of probability that a serious crime will be committed.

Cameroon's MTN Twitter shutdown can also be seen as a reminder that we lack both judicial and legislative mechanisms to protect people from unlawful government surveillance. Then, what are the reactions of different stakeholders since "the same rights that people have offline must also be protected online"?[13]

Officials have always been wary about the internet and other social networks, for they allow individuals to express their ideas and opinions directly to a world audience, and easily to each other. Since the Arab Spring – and mostly in Africa – the possibility of the internet and social media networks empowering citizens and the media in mobilisation is considered a real threat by some governments. However, civil society has so far paid little attention to the issue of surveillance, given that very few cases have been reported. Communications surveillance is also disconnected from the daily concerns of the Cameroonians, given that only 5% of the population are internet users.

Finally, MTN is a South African-based mobile operator, and although this report does not address this issue directly, the complicity of foreign companies colluding in state monitoring activities needs to be addressed.

Action steps

With the increasing sophistication of information technology, concerns over privacy violations are now greater than at any time in recent history. So it

10 UN Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet", Resolution 20 (2012), UN Doc A/HRC/20/L.13.

11 Reporters Without Borders. (2011, March 22). Government blocks Twitter via SMS service. *IFEX*. www.ifex.org/cameroon/2011/03/25/twitter_blocked

12 Communications surveillance might also endanger the social peace, as was the case in Cameroon some two years ago when WikiLeaks, the famous leaks website, reported the tribalist statements of former justice minister Amadou Ali regarding President Paul Biya's succession.

13 According to the resolution adopted on 5 July 2012 by the UN Human Rights Council.

is legitimate to express fears about a possible encroachment on privacy. Therefore, we suggest the following action steps in Cameroon:

- Laws that already exist that protect the rights to freedom of expression and privacy should be implemented in order to prevent abuse of emergency powers that can shut down networks or intercept communications.
- Cameroon's parliament must appoint an intelligence and security committee to oversee intelligence and security activities that reports directly to parliament.
- Parliament could also appoint an independent intelligence service commissioner and a communications interception commissioner among former senior judges whose reports, once again, should be addressed directly to the parliament.
- Legal safeguards to limit the scope and determine the grounds of possible surveillance and institutions and officials competent to authorise and carry out communications surveillance should be developed.
- The National Commission on Human Rights and Freedoms should be empowered to make sure that surveillance occurs only as provided in law, that it occurs only when necessary and that it is proportionate to the aim being achieved.
- The government must communicate with the public on how it uses its surveillance powers. This reporting should include the number of data requests made to telecommunications operators and to other mobile and internet service providers, and the number of individuals or accounts that were implicated.[14]
- The developers of surveillance tools should take immediate steps to address their misuse. This may require them to be more transparent, and to develop internal company policies against misuse by governments or other stakeholders.

14 Human Rights Watch. (2014). *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*. www.hrw.org/reports/2014/03/25/they-know-everything-we-do « *they know everything we do* »