Ms Kate Fox
Secretary
UN Human Rights Committee
Office of the United Nations
High Commissioner for Human Rights
UNOG-OHCHR
1211 Geneva 10, Switzerland

New York, 20 September 2017

Dear Ms. Fox,

Re: Submission to the UN Human Rights Committee on Concerns and Recommendations on Cameroon

Access Now and Internet Sans Frontièrs welcome the upcoming review of Cameroon by the Human Rights Committee. This briefing provides an overview of our main concerns with regard to Cameroon's compliance with the International Covenant on Civil and Political Rights (ICCPR). We hope it will inform the Committee's pre-sessional review of Cameroon and that the areas of concern highlighted here will be reflected in the list of issues submitted to the Cameroonian government ahead of the review.

Violations of freedom of expression (Article 19)

The Cameroonian government has explicitly expressed its contempt for freedom of expression online. On October 2016, the Minister of Transports accused social media networks of enabling rumor-mongering and the Minister of Communications, the spokesperson for the government, labeled social media a threat to peace. On November 2016, the President of the National Assembly labeled internet users as "traitors of the cyberspace" and social media participants as "terrorists". In 2017, the government used telecom companies to send text messages to subscribers threatening up to two years in prison if they used social media to spread rumors and false news[1].

On January 17, 2017, the government ordered the suspension of internet services in the Northwest and Southwest anglophone regions of Cameroon. The shutdown lasted 94 days and adversely impacted the region's 5 million residents. For three months, the shutdown went nearly unacknowledged by the Cameroonian government or mobile phone companies. Yet the evidence shows that the government ordered telecommunications companies to shut down internet access in anglophone regions. A recorded phone conversation with a senior MTN executive indicates that companies received explicit instructions from the government to block

[1] Julie Owono,'Cameroon's reflection on the "false news" debate stirs censorship fears' (Internet Sans Frontiers, 21 November 2016) <https://internetwithoutborders.org/fr/cameroonian-governments-dangerous-stance-against-a-free-and-open-internet/> accessed August 1, 2017

internet connectivity as a condition of their license agreements[2]. A letter from Cameroon Telecommunications (CAMTEL), Cameroon's national telecommunications company, to the minister for post and telecommunications confirms that the company "coercively enforced" the government's instructions to suspend internet services "in certain sensitive regions"[3]. Two months into the shutdown, following a call to action[4] from Access Now, Orange Cameroon responded stating that it "complies with the local legislation and therefore obeys to any national security instruction received from the authorities in accordance with its Telecommunications License[5]."

The international community labels this type of blocking of telecommunications networks and services as an "internet shutdown." A growing body of jurisprudence declares shutdowns to violate international human rights protections of freedom of speech. In 2015, experts from the United Nations (UN) Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR), issued an historic statement declaring that internet "kill switches" can never be justified under international human rights law, even in times of conflict[6]. In 2016, the Human Rights Council referred to internet shutdowns in its consensus Resolution 32/13, which "*condemns unequivocally* measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures"[7]. Thus, this government-ordered shutdown constitutes a violation of Article 19 of the ICCPR.

Targeting of Anglophone regions (Articles 21 and 27)

The internet outage was the culmination of months of protests against the dominance of French-language use in courts and schools in the predominantly English speaking region. These protests escalated into clashes with the police in which at least four were killed and many others were injured. During the same period, students of the University of Buéa in the Southwest protested against financial penalties for late tuition payments. Students then took to social

---

[2] Cameroon. "1248776918531895." SoundCloud audio, 8:47, February 2017. https://soundcloud.com/ameroon.

[3] @Dbergeline. Twitter Post. 21 January 2017 (5:28 PM).https://twitter.com/Dbergeline/status/822798121688305665/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fqz.com%2F893401%2Fcameroon-pressured-mtn-and-other-operators-to-shut-down-internet-in-bamenda-buea-regions%2F

[4] "Open letter to telecommunications companies in Cameroon on the internet shutdown" (Access Now, 15 February 2017), https://www.accessnow.org/open-letter-telecommunications-companies-cameroon-internet-shutdown/

[5]Orange (France), 14 March, 2017, https://business-humanrights.org/sites/default/files/documents/Orange%27s%20response-14-March-2017.docx

[6] Peter Micek, (Access Now 4 May 2015) 'Internet kill switches are a violation of human rights law, declare major UN and rights experts' <https://www.accessnow.org/blog/2015/05/04/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un>

[7] A/HRC/RES/32/13 (18 July 2016), available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13>.

media to document evidence of police brutality[8]. In response, the Cameroon Anglophone Civil Society Consortium (CACSC) and Southern Cameroons National Council (SCNC) led "Ghost Town" strikes, during which they asked members of the public to stay at home and shops and businesses to close. On the same day these organizations were banned the internet was shut off.

The internet blackout created "internet refugees", as anglophone Cameroonians were forced to travel into francophone regions or Nigeria to get internet access. The "Silicon Mountain", which is located in the affected region, was especially crippled by the loss of internet. According to the figures of independent organization, no fewer than 200 young entrepreneurs were unemployed as their businesses were halted by the shutdown and they were unable to find work in the major French-speaking metropolises like Douala. After weeks of commuting to the almost 74 km from Buea to the commercial capital of Douala to access the internet, tech developers built and internet "refugee camp" in Bonako, a village near the toll gate separating the Southwest from the Francophone region of Littoral[9].

Research shows that internet shutdowns and human rights infringements go hand-in-hand[10]. Shutdowns disrupt the free flow of information and create a cover of darkness that allows state and non-state actors to persecute vulnerable groups without scrutiny. Moreover, Maina Kiai, UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, has affirmed (at para. 75) the significance of internet access to the right to free assembly, recognizing the importance of organizations' ability to use communication technologies securely and privately to their ability to operate effectively[11]. Any restriction to online access must be necessary and proportionate, and there must be adequate safeguards against abuse. The targeting of majority-anglophone regions in order to silence protests from English-speaking Cameroonians breaches both Article 21's requirement of freedom of association and Article 27's protection of linguistic minorities.

Violations of privacy (Article 17)

Recent legislation has allowed the government to violate online privacy with little oversight. The 2010 Cybersecurity and Cybercriminality law includes measures that permit the immediate identification of internet users without sufficient safeguards against abuse of power and invasion of privacy:

---

[8] Awah (pseudonym), 'Students in Cameroon beaten and intimidated for protesting' (France 24, 1 December 2016), http://observers.france24.com/en/20161201-students-cameroon-beaten-humiliated-protesting

[9] Abdhi Latif Dahir, 'Reeling from an internet shutdown, startups in Cameroon have created an "internet refugee camp' (Quartz Africa, 28 March 2017), <https://qz.com/942879/an-internet-shutdown-in-cameroon-has-forced-startups-to-create-an-internet-refugee-camp-in-bonako-village/>

[10] Sarah Myers West, 'Research Shows Internet Shutdowns and State Violence Go Hand in Hand in Syria' (Electronic Frontier Foundation, 1 July 2015) <https://www.eff.org/deeplinks/2015/06/research-shows-internet-shutdowns-and-state-violence-go-hand-hand-syria> accessed 18 February 2016.

[11] United Nations, Human Rights Council, *Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies,* A/HRC/31/66 (4 February 2016), available from undocs.org/A/HRC/31/66.

1. Section 25 requires network operators, internet service providers (ISPs) and operators of information systems to retain traffic data of their users for at least 10 years. Access, service, and content providers must also retain data which allows it to identify users for 10 years. This is much longer than the average time companies hold on to this data for business purposes, and the justification and objective of this data retention is not defined. These provisions pose serious risks to users' privacy, as retaining large stores of sensitive user data increases risk of breach by malicious attackers, misuse by staff, or unlawful access by government officials.
2. Section 92 gives broad powers to various authorities in charge of implementing the law: police officers can intercept, record or transcribe any electronic communication without having to respect the rules of the Cameroonian Penal Procedure Code. Some offenses such as spreading false news - which is broadly defined by the law - enable police to implement the measure, which seriously violate citizens' privacy.
3. Section 26 provides that “operators of information systems assess, review their security systems and introduce, if necessary, the appropriate changes in their practices, security measures and techniques according to the evolution of technology.” These provisions could be interpreted to permit operators of information systems to introduce backdoors in the systems they are supposed to secure.
4. Section 55 of the cybersecurity law also requires encrypted, encoded and compressed data to be handed over to authorities upon request. Private keys must also be delivered on request of regulated agents and, if they are not available, the judicial authorities may appoint an expert to "perform technical operations to obtain the clear version of said data." The law allows authorities to appeal to a hacker to decipher an encrypted communication, possibly for any procedure. These provisions pose significant risks to the privacy of users, and do not fit the requirements of necessity and proportionality imposed by international law.
5. Section 83 makes it a crime to propose sex to a person of the same sex by way of electronic communications, and conviction carries a prison sentence of up to 2 years and a fine up to 1 million CFA francs. Cameroonian law plans to double these penalties when the proposals are followed by sex. These provisions are clearly detrimental to respect for individuals' privacy, and pose a risk to people whose rights are already precarious in the physical space. In combination with Law No. 2010/012, they create chilling effects and threaten lawful expressive activity, association, and privacy, among other human rights.

Recent news from Cameroon give examples of how the vagueness of the law allows privacy violations. In April 2017, after the government restored internet access to anglophone regions of Cameroon, the Minister of Post and Telecommunications admitted that the country was implementing surveillance programs to monitor activities of citizens online[12]. On 19 March 2014, the general manager of the ANTIC (Agence Nationale des Technologies et l’Information de la Cameroun) gave an interview to the government’s daily newspaper Cameroon Tribune detailing how social media and websites are monitored in Cameroon. He revealed that the ANTIC uses a technical platform that searchers for profiles on social networks using keywords to detect “illicit content representing a potential threat for the national security and the image of Cameroon,”

[12] Julie Owono, “Internet back in anglophone Cameroon, but more surveillance?” 25 April, 2017, https://internetwithoutborders.org/fr/internet-back-in-anglophone-cameroon-but-more-surveillance/

including those that incite hatred or are slanderous.[13] Such social media monitoring interferes with fundamental rights, and should only occur under impartial judicial oversight, when necessary and appropriate to strictly achieve a legitimate aim.

About **Access Now**

Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world, including engagement with stakeholders and policymakers in Cameroon, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
Access Now advocates an approach to digital security that promotes good security policies that protect user rights, including privacy and freedom of expression. Access Now has worked extensively to draw attention to digital rights in Cameroon, including commenting on the January 2017 internet shutdown.

About **Internet Sans Frontières (Internet Without Borders)**

Internet Sans Frontières is a non profit organization with the non-profit status under French law. The organization promotes and defends freedoms in the digital space, including freedom of expression and the right to privacy, and an open web accessible to all, without discrimination.

For more information, contact:

Peter Micek

General Counsel | Access Now

peter@accessnow.org | +1-888-414-0100 x709

Julie Owono

Executive Director | Internet Sans Frontières

julie@internetsansfrontieres.org

[13] Serge Daho, Sylvie Siyam,'The stammerings of Cameroon's communications surveillance' (Global Information Society, 2014) ,https://giswatch.org/en/country-report/communications-surveillance/cameroon>