**EXPRESSION OF INTEREST**

**TECHNICAL CONSULTANT TO CARRY OUT A PERCEPTION SURVEY: IMPACT OF COMMUNICATION SURVEILLANCE ON HUMAN RIGHTS DEFENDERS IN KENYA**

## WHO WE ARE

The National Coalition of Human Rights Defenders–Kenya (NCHRD-K) is a national organization incorporated in the Republic of Kenya as a Trust. Its mission is to strengthen the capacity of human rights defenders (HRDs) to work effectively in the country and to reduce their vulnerability to the risk of persecution, through protection, capacity building, and advocacy for a favourable legal and policy environment. Established in 2007, NCHRD-K is the only national organisation that works primarily for the protection of HRDs.

## BACKGROUND

HRDs play a critical role in the realization of human rights in the world. Consequently, they face reprisals ranging from intimidation, threats, physical assault and even death. Their demand for accountability and transparency from perpetrators of human rights violations, and speaking truth to power puts them at odds with the powerful elite in society who threaten the civic space in which HRDs and civil society organizations operate.

The government has put in place numerous measures to limit the space for civil society and HRDs. These include legal restrictions, administrative actions, malicious prosecution, limitation of fundamental freedoms of association, assembly and expression as well as summary execution. Most recently, with the increased reliance on technology, the violation of the right to privacy through surveillance has become more prevalent.

The right to privacy is a fundamental human right recognized under international law under Article 17 of the International Covenant on Civil and Political Rights and also enshrined in the Constitution of Kenya under Article 31. The right to Privacy is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association. However, the right to privacy is not an absolute right. Activities that restrict the right to privacy can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[1]

[1] Article 24 Constitution of Kenya

Following the terror attacks on Kenya, including the Westgate mall attack and the Garissa University terror attack, the Government put in place numerous measures in an attempt to mitigate against the same. These included increased surveillance with the State seeking access to both communications content without adequate scrutiny. The Kenyan government has on a number of occasions alluded to their conduct or attempted conduct of communication surveillance and even put in place measures that enable surveillance.

In 2010, the Communication Commission of Kenya (CCK), now the Communications Authority of Kenya, the government telecommunications regulator, announced that mobile phone subscribers would be required to register their details with operators or risk having their Subscriber Identity Module (SIM) cards deactivated.[2]

In March 2012, the Communications Commission of Kenya (CCK), announced that it was setting up a system to allow the authorities to monitor incoming and outgoing digital traffic. In November 2014, the government contracted Kenya's largest mobile service provider Safaricom to develop a secure communication and surveillance system, known as the National Command Control and Communication (IC3) Centre)[3], to boost the capacity of the country's national security agencies to fight terrorism.

In June 2015, the Communications Authority of Kenya (CA) Director-General Francis Wangusi in 2015 stated that the CA was drafting legislation that would require anyone accessing wireless internet through public hotspot to register their devices with the service provider, as part of the government effort to crack down on cybercrime.[4] Later in 2017, the CA stated that the state agency had acquired surveillance systems to monitor social media and mobile phones during the elections and that internet shutdown would only be used in the "worst-case scenario."[5]

Although Kenyan law requires judicial approval for the interception of communications and permits the limitation of privacy only by an Act of Parliament, the Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations grant extensive powers to state authorities to collect and access the data of mobile phone users. Such access enables the government to know one's communication pattern and even location making individuals vulnerable to physical surveillance and at worst summary execution.[6]

---

[2] Communications Commission of Kenya, It's now mandatory to register your SIM card, 21 June 2010. Available at: http://www.cck.go.ke/news/2010/news_21june2010.html

[3] https://freedomhouse.org/report/freedom-net/2015/kenya; http://www.itnewsafrica.com/2015/05/kenyas-safaricom-says-national-police-surveillance-system-live/

[4] CA rule to require registration for use of public Wi-Fi, http://www.businessdailyafrica.com/CA-rule-to-require-registration-for-use-of-public-Wi-Fi/539546-2771074-12uvfod/index.html June 2015

[5] Kenya may 'block internet' during elections http://www.bbc.com/news/live/world-africa-38235211

[6] Track Capture Kill, Privacy International, https://privacyinternational.org/sites/default/files/track_capture_final.pdf

There are concerns with the above-mentioned initiatives, and that judicial oversights are being circumvented, thus violating the right to privacy. This poses concerns as to the safety and security of sensitive information held and communicated by HRDs in the course of their human rights work. They are thus reduced to self censorship and fear of engaging in their human rights work.

**PURPOSE AND OBJECTIVE OF THE STUDY**

This study aims to undertake a thorough assessment to better understand the needs, concerns and areas of interests of HRDs in relations to privacy, data protection and communications surveillance in particular with regards on how these impact their work and their role as actors of change in society.

This study also aims to inform the development of intervention strategies by NCHRD-K for HRDs at risk, to build on NCHRD-K's already existing digital security curriculum, using the results of the report as an advocacy tool.

To these aims, the study will seek to:

- assess HRDs' level of exposure, understanding and perception of communication surveillance;
- identify HRD's strategies for mitigating against communication surveillance.

**TASKS AND RESPONSIBILITIES OF THE CONSULTANT**

The consultant will:

- Conduct desk review/ review of existing literature, including but not limited to case studies on the subject matter;
- Conduct field work
- Convene one-on-one interviews and focus group discussions with HRDs
- Analyze and compile data collected from the field study;
- Compile a draft report to be shared with the NCHRD-K and partners for review and input; and
- Compile a final report incorporating feedback from NCHRD-K and partners.

**APPROACH OF THE SURVEY**

The survey is will be conducted at the community and national level through one-on-one interviews and focus group discussions with HRDs from preselected regions based on the thematic areas of focus and the prevailing environment in the particular counties.

**KEY DELIVERABLES**

Upon completion the consultant shall submit to NCHRD-K:

1. All raw data collected in the course of the exercise including any notes relevant to the

work.

2. Inception report (final survey instrument and methodology, as well as date-specific timeframe for data collection, analysis and final report)
3. Final report of findings.

**TIME-FRAME**

The consultant must be ready to start work immediately upon appointment. The maximum number of days allowable for the consultancy work shall not exceed thirty (30) working days.

**PROFILE AND EXPERIENCE OF CONSULTANT**

Candidates for this consultancy should possess the following minimum qualifications:

- Demonstrated understanding of issues related to privacy, data protection, communications and/or human rights and technology
- Proven and demonstrable relevant experience working on Privacy and surveillance or HRD related issues.
- Proven and demonstrable relevant experience on not less than five (5) years in safety and protection issues.
- Proven and demonstrable relevant experience of conducting surveys (preferably perception surveys), undertaking interviews and focus group discussions, and conducting data analysis.
- Extensive knowledge on the Constitution of Kenya 2010 and international and regional legal instruments that protect the rights of human rights defenders, freedom of expression and right to privacy.
- Demonstrable experience producing materials of similar nature.
- A minimum qualification of a Degree in law, political science, policy analysis or other related field
- Fluency in English and Kiswahili

**Application Procedure**

Interested consultants must include in their application the following:

1. **Technical Proposal not exceeding 5 pages on:**

- An understanding and interpretation of the TOR
- Methodology to be used in undertaking the assignment
- Time and activity schedule

2. **Financial proposal not exceeding 1 page**

- Consultant's daily rate in Kenya Shillings
- Other costs e.g. travel, accommodation
- Total cost

3. **Organizational and Personnel Capacity Statement**

- Relevant experience related to the assignment (include samples of two most recent similar works and/or references for the same)
- Contacts of at least 3 organizations previously worked for.
- Curriculum Vitae of the Consultant(s).

**SUBMISSION OF PROPOSAL**

Interested and qualified consultants should submit their application to advocacy@hrdcoalition.org with the subject **"TECHNICAL CONSULTANT APPLICATION"** on or before **10 October 2017.**