The Right to Privacy in Kenya

Stakeholder Report
Universal Periodic Review
21st Session - Kenya

Submitted by Privacy International and the National Coalition of Human Rights Defenders in Kenya (NCHRD-K)

June 2014

Introduction

1. This stakeholder report is a submission by Privacy International (PI) and the **National Coalition of Human Rights Defenders** in **Kenya (NCHRD-K). PI** is a human rights organisation that works to advance and promote the right to privacy around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged. **NCHRD-K** is a non-governmental organisation registered as a Trust in Kenya. It was established to strengthen the work of human rights defenders (HRDs) in the country by reducing their vulnerability to the risk of persecution and by enhancing their capacity to effectively defend human rights. The founding of the National Coalition was informed by a number of issues and challenges that HRDs faced individually in the course of their work that called for better collaboration and support.

2. Together PI and NCHRD-K wish to bring their concerns about the protection and promotion of the right to privacy in Kenya before the Human Rights Council for consideration in Kenya's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

individuals.[2] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3]

4. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[4] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

Follow up to the previous UPR

5. There was no mention of the right to privacy and data protection neither in the National Report submitted by Kenya nor in the report of the Working Group. On the other hand, stakeholders raised widespread concerns regarding the right to freedom of expression and attacks against HRDs and journalists. The Working Group made several relevant recommendations to the Kenyan government on these issues, including:[7]
   - Take every useful measure to investigate human rights violations committed by the police, in particular extrajudicial killings, in order to bring to justice the perpetrators of such acts and ensure the effective protection of HRDs and witnesses (France) – Recommendation 101.43;
   - Review its national legislation on freedom of expression so that it fully complies with the relevant provisions of the International Covenant on Civil and Political Rights, and ensure the effective protection of HRDs against harassment or persecution (Czech Republic) - Recommendation 101.87;
   - Promptly take effective measures to safeguard the work of HRDs, including by ensuring that witness protection and the

[2] Martin Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 2009, A/HRC/17/34.
[3] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.
[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).
[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)
[6] As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416
[7] Human Rights Council, *Report of the Working Group on the Universal Periodic Review: Kenya, Fifteenth session, Agenda item 6*, Universal Periodic Review, 17 June 2010, A/HRC/15/8. Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/144/88/PDF/G1014488.pdf?OpenElement

protection of HRDs who assist witnesses are a priority for the Government (Sweden) - Recommendation 101.88;

- Investigate harassment and attacks against journalists and HRDs in order to bring those liable to justice (Norway) - Recommendation 101.89;

International obligations related to privacy

6. Kenya is a signatory to the Universal Declaration of Human Rights ('UDHR') and has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "*adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy].*"[8]

7. **Article 2** of **Kenya's Constitution** states:

> *"(5) The general rules of international law shall form part of the law of Kenya.*
>
> *Sovereignty of the people.*
> *(6) Any treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution."*

Domestic laws and regulations related to privacy

8. **Article 31** of the **Constitution of Kenya**[9] protects the rights to privacy. It states:

> *Every person has the right to privacy, which includes the right not to have—*
> *(a) their person, home or property searched;*
> *(b) their possessions seized;*
> *(c) information relating to their family or private affairs unnecessarily required or revealed; or*
> *(d) the privacy of their communications infringed.*

9. **2009 Kenya Information And Communications Act**, includes the following provisions:

> **Article 31**

[8] General Comment No. 16 (1988), para. 1
[9] Available at: http://www.parliament.go.ke/plone/national-assembly/the-constitution/constitution-2010/TheConstitution_of_Kenya_2010.pdf

"A licensed telecommunication operator who otherwise than in the course of his business—

(a) intercepts a message sent through a licensed telecommunication system; or

(b) discloses to any person the contents of a message intercepted under paragraph ; or,

(c) discloses to any person the contents of any statement or account specifying the telecommunication services provided by means of that statement or account, commits an offence and shall be liable on conviction to a fine not exceeding three hundred thousand shillings or, to imprisonment for a term not exceeding three years, or to both."

Article 83 W

(1) Subject to subsection (3), any person who by any means knowingly:—

(a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, shall commit an offence.

Article 93 (1)

No information with respect to any particular business which—

(a) has been obtained under or by virtue of the provisions of this Act; and

(b) relates to the private affairs of any individual or to any particular business,

shall, during the lifetime of that individual or so long as that business continues to be carried on be disclosed by the Commission or by any other person without the consent of that individual or the person for the time being carrying on that business.

10. **Section 15 (1)** of the **Kenya Information And Communications (Consumer Protection) Regulations, 2010**, states that,

"Subject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data."

Areas of Concern

1. Communications surveillance

11. Despite Kenya's efforts to strengthen and embed protection of privacy both in its constitutional and legislative framework, there are increasing concerns over certain surveillance practices and policies, such as the adoption of the Prevention of Terrorism Act 2012, the Network and Early Warning systems (NEWS) in 2012, and the Integrated Public Safety Communication and Surveillance System in May 2014. These measures are often framed within government strategies to combat terrorism, cyber criminality, fraud and corruption. A group of Kenyan and international organisations including Human Rights Watch, Amnesty International and Open Society Justice Initiative have expressed concerns over reports of human rights violations by the Kenyan security forces in the context of counterterrorism operations. These have included threats against HRDs and journalists for exercising their right to freedom of expression[10].

12. In a report presented at the 23rd session Human Rights Council in May 2013, Frank La Rue, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, drew attention to the interlinking relationships between the right to freedom of expression, the right to privacy and surveillance.[11] The report pointed to the need to further study new modalities of surveillance and recommended the revision of national laws regulating these practices to bring them into line with human rights standards. Mr La Rue's concerns gained particular salience following the revelations of NSA whistle-blower Edward Snowden from June 2013 onwards. Various UN bodies including the UN General Assembly[12], the Human Rights Council[13] and the High Commissioner for Human Rights[14], have

[10] Human Rights Watch, *Joint Letter to the ACHPR Regarding Violations in the Context of Kenyan Counterterrorism Operations*, 12 May 2014. Available at: http://www.hrw.org/news/2014/05/29/joint-letter-achpr-regarding-violations-context-kenyan-counterterrorism-operations

[11] 1 A/HRC/23/40, 17 April 2013. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[12] In November 2013, the Third Committee of the General Assembly approved a resolution titled "Right to Privacy in the Digital Age". The UN General Assembly voted unanimously the resolution on 18 December 2013. In this Resolution, the General Assembly is calling upon Member States to review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data, including mass surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law.

[13] The 24th Session of the UN Human Rights Council in September 2013 included a side-event on privacy in the digital age hosted by the governments of Germany, Norway, Austria, Hungary, Liechtenstein and Switzerland during which the International Principles on Application of Human Rights to Communications Surveillance were launched.

addressed the right to privacy and its relationship with state surveillance.

13. Technologies with capacities to conduct surveillance and monitoring as well as intrusive and sophisticated surveillance programmes (such as those outlined below) are incredibly powerful tools in the hands of governments and potentially subject to serious abuse. 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. There are concerns that judicial processes are being circumvented and the privacy of citizens violated.

a. Surveillance and monitoring systems

14. In March 2012, the telecommunications industry regulator, the Communications Commission of Kenya (CCK), announced[15] it was setting up a system to allow the authorities to monitor incoming and outgoing digital communications. CCK requested that all telecommunication service providers cooperate in the installation of internet traffic monitoring equipment; known as NEWS. The CCK cited a rise in cyber security threats as a justification for this move. NEWS is an initiative of the UN's International Telecommunication Union (ITU)[16] and is presented as a tool to identify threats and provide advice on how to respond. When it was announced internet service providers, civil society organisations (CSOs) and the legal community expressed concerns about this initiative as it appeared to contravene Article 31 of the Kenyan Constitution which protects the right to privacy, in particular paragraph (d) which upholds individuals' right not to have "*the privacy of their communications infringed.*"[17]

15. In January 2013, the Citizen Lab of the University of Toronto published a research brief[18] in which it reported that

---

[14] In July 2013, following revelations about the operation of the National Security Agency of the United States of America, leaked by Edward Snowden, the High Commissioner for Human Rights, Navi Pillay stated: "*While concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programmes, surveillance without adequate safeguards to protect the right to privacy actually risk impacting negatively on the enjoyment of human rights and fundamental freedoms.*"

[15] Communications Commission of Kenya, Kenya and ITU sign administrative agreement for KE-CIRT/CC, 17 February 2012. Available at: http://www.cck.go.ke/news/2012/KE-CIRT_signing.html

[16] ITU News, Making an IMPACT on global cybersecurity, October 2009, Available at: https://www.itu.int/net/itunews/issues/2009/08/22.aspx

[17] Okuttah, M., CCK sparks row with fresh bid to spy on Internet users, Business Daily, 20 March 2012. Available at: http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/x6adjmz/-/index.html

[18] CitizenLab, *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Research Brief, Number 13, January 2013, University of Toronto, MUNK School of Global

researchers had discovered three Blue Coat PacketShaper installations[19] in various countries including Kenya. Blue Coat allows the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter, Google Mail, and Skype.[20] Whilst such tools can be used for legitimate aims, such as controlling bandwidth costs, they also have the functionality to permit filtering, censorship, and surveillance. Although there is no evidence as to whether Blue Coat PacketShaper installations were implemented in Kenya, the announcement in 2012 of the establishment of the NEWS system outlined above, and the presence of these installations in Kenya raises concerns as to the potential surveillance capacities of the Kenyan government and the purposes for which they might be deployed.

16. In May 2014, the government announced[21] that the partially-state owned Kenyan telecommunications agency Safaricom had been awarded a government tender to set up a new telecommunications surveillance system for the Kenyan Police, known as the *Integrated Public Safety Communication and Surveillance System*. However in June 2014, the Kenyan National Assembly's Committee on National Security decided to suspend this new system on the basis that the procurement process had failed to meet necessary standards. There is an on-going legal battle over the tender process.[22] At the time of submitting this joint stakeholder report, no decision had been made as to which company would be awarded the tender.

17. When the surveillance system was made public, it was announced that the system would cost KES 12.3 billion (approximately USD 140 million). There are two elements to the project. First, the system would link-up all security agencies in order to facilitate information sharing and operationalisation of activities. Secondly, it would establish an expensive surveillance camera system consisting of 1800 CCTV cameras.

Affairs. Available at: https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf

[19] Ibid, pp. 25. *"All three were initially identified by Shodan in December 2012 and were verified as accessible. These were on netblocks associated with Hughes Network Systems, which is a satellite-based Internet provider. The hostnames of the IP addresses of these installations resolve to the iWayAfrica domain, which is an African provider of broadband Internet service."*

[20] *Applications that Blue Coat PacketShaper Classifies and Controls*. Available at: http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf

[21] Press Statement by His Excellency Honorable Uhuru Kenyatta, C.G.H., President And Commander-In-Chief Of the Defence Forces of the Republic of Kenya on 16th May 2014 at State House Nairobi. Available at: http://www.president.go.ke/press-statement-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-on-16th-may-2014-at-state-house-nairobi/

[22] Shiundu, A., *House Committee suspends national surveillance system deal*, Standard Media, 5 June 2014. Available at: tp://www.standardmedia.co.ke/article/2000123706/house-committee-suspends-security-surveillance-system-deal?articleID=2000123706&story_title=house-committee-suspends-national-surveillance-system-deal&pageNo=1

These would be installed in Nairobi and Mombasa and connected to 195 police stations in those two cities through an independent 4G network to keep them connected in real time. The camera surveillance infrastructure would permit facial and movement recognition in real time through the transfer of camera footage to a monitoring centre. A monitoring centre is a centralised system where data collected from various points of interception is collected, retained and analysed. The Nairobi aspect of the project was expected to be completed by the end of 2014, whilst the Mombasa operation was expected to take 18-24 months. These time frames may be revised given the delay in the project, and the fact that the tender awarded to Safaricom is being revised.

18. It is not yet clear who will be responsible for its operationalisation or even if it will be implemented but the privacy implications of this system are numerous and significant. Key concerns include the possibility of data sharing with third parties (including foreign agencies and the private sector), the processing and collection of communications and images without the consent of individuals, the risks of insecure storage facilities and unauthorised external access, and the potential for data to be deleted or modified.

19. The Intercept reported on 19 May 2014[23] that a NSA programme called MYSTIC secretly monitors the telecommunications systems of several countries including Kenya, where the system is known as DUSKPALLET. The programme was described in internal NSA documents as a *"program for embedded collection systems overtly installed on target networks, predominantly for the collection and processing of wireless/mobile communications networks."*[24] Evidence provided to The Intercept shows that the programme dates back to 2013, and that data gathered through it has been used to generate intelligence reports. The Intercept states that *"the operation in Kenya is 'sponsored' by the CIA, according to the documents, and collects 'GSM metadata with the potential for content at a later date'."*[25] In some of the other countries where MYSTIC is implemented (Bahamas, Mexico and the Philippines) MYSTIC required "contracted services for its 'operational

[23] Devereaux, R., Greenwald, G., and Poitras, L., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, The Intercept, 19 May 2014. Available at: https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

[24] See: https://www.documentcloud.org/documents/1164087-mystic.html , Slide published by The Intercept *The Intercept, Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

[25] SSO Dictionary Excerpt https://firstlook.org/theintercept/document/2014/05/19/sso-dictionary-excerpt/ published by *The Intercept, Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

sustainment'"; this is not the case for Kenya, however.[26] Therefore it is unclear what and if any role the government of Kenya as well as telecommunication and communication providers played in the deployment of MYSTIC. These revelations support the need for the implementation of strong data protection standards to ensure that the Kenyan government meets its international legal obligations to protect the privacy of its citizens.

b. Access to communications data

20. Under section 31 of the Kenya Information and Communication Act, licensed telecommunication operators are legally prohibited from implementing technical requirements necessary to enable lawful interception, and section 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010, states that a licensee (licensed under the KIC Act) *"shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data".*

21. However, the recently adopted Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2014[27] permit access to private or confidential information on consumers without a court order. Section 13 reads:

> *"A licensee[28] shall grant the Commission's officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations."*

22. The obligation the regulations place on telecommunications service providers to provide access to their systems without a court order violates the right to privacy.

---

[26] Devereaux, R., Greenwald, G., and Poitras, L., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, The Intercept, 19 May 2014. Available at: https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

[27] Legal Notice No. 10 to the Kenyan Communications and Information Act, 7 February 2014. Available at: http://kenyalaw.org/kl/index.php?id=4215

[28] Means a person or entity licensed under the Act to own and operate a telecommunication system or to provide telecommunication services or both

23. Vodafone's transparency report, Law Enforcement Disclosure Report[29], published In June 2014, revealed that it had *"not received any agency or authority demands for lawful interception assistance"*[30] in Kenya. The inference from this disclosure is that the Kenyan authorities have direct access to Vodafone's network, which allows the government to monitor communications directly without having to go to the company to seek the data of their customers.[31] This type of unfettered access permits uncontrolled mass surveillance of Vodafone's customers and anyone in contact with those customers, which amounts in a direct unlawful interference with the right to privacy.

c. Limiting access to internet and mobile services

24. During and in the aftermath of the March 2013 elections, the Kenyan government requested that mobile phone providers block text messages that were deemed to incite violence using a firewall that would detect messages containing key words, identified beforehand, to be further analysed.[32] The National Steering Committee on Media Monitoring of the Ministry of ICTs intercepted 300,000 texts messages during the 2013 elections. [33] This practice shows the extensive power the government exercises over telecommunication and internet providers and their operations.

d. Lack of oversight

25. The Kenya National Intelligence Agency (NIS) was established by the 2012 National Intelligence Service (NIS) Act, and is both the domestic and foreign intelligence agency of Kenya.

26. Article 36 reads:

> *"(1) The right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with.*

---

[29] Vodafone, *Law Enforcement Disclosure Report – Country-by-country section*, pp. 61-80, in *Sustainability Report 2013/14*. Available at: http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf

[30] Ibid, pp. 77

[31] Ibid, pp. 69

[32] Freedom House (2013) *Freedom on the Net 2013: Kenya*. Available at: http://www.freedomhouse.org/report/freedom-net/2013/kenya#.U3y3TFhdU00

[33] Kenya Human Rights Commission, *The Internet Legislative and Policy Environment In Kenya*, January 2014, pp. 14. Available at: http://www.khrc.or.ke/resources/publications/doc_details/67-the-internet-legislative-and-policy-environment-in-kenya.html

(2) The Service shall, prior to taking any action under this section, obtain a warrant under Part V."

27. Article 45 states:

> *"….an officer of the Service the power to obtain any information, material, record, document or thing and for that purpose –*
> *(a) to enter any place, or obtain access to anything;*
> *(b) to search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing;*
> *(c) to monitor communication; or*
> *(d) install, maintain or remove anything."*

28. Kenya lacks legislation to appropriately regulate the powers of public bodies to carry out surveillance. Instead, Article 35 of the Prevention of Terrorism Act 2012 grants extensive powers to state authorities to limit fundamental freedoms and encroach on the right to privacy through surveillance. In view of the 2013 terrorist attack on the Westgate shopping mall, the Act has been presented as a positive tool to tackle threats to national security.

29. Based on accountability documents submitted to Parliament[34], President Kenyatta plans to review the Prevention of Terrorism Act to include: a "shake-up" of the NIS, better protection for Kenyans, publication of the security budget to promote transparency, the elimination of wastage, the inclusion of a guarantee of quality and value for public funds, and better protection of Kenyans. If this programme is carried out, it is important that reforms will not come at the expense of individuals' privacy and other fundamental freedoms.

30. Without adequate regulation and oversight of communication monitoring and surveillance programmes, the Kenyan intelligence agencies are failing to ensure that their policies and practices adhere to international human rights standards and adequately protect the rights to privacy and freedom of expression. *The International Principles on the Application of Human Rights to Communications Surveillance*[35] provide guidance and structure for

[34] State of the Nation Address at Parliament by H.E. President Uhuru Kenyatta, 27 March 2014. Available at: http://www.president.go.ke/state-at-the-nation-address-at-parliament-by-h-e-president-uhuru-kenyatta/

[35] Launched in September 2013 following a year of consultation, the International Principles on the Application of Human Rights to Communications Surveillance a set of standards that interpret States' human rights obligations in light of new technologies and surveillance capabilities. The Principles are endorsed by 410 civil society organisations around the world, over 40 leading experts, academics and prominent individuals, as well as 4 elected officials. The Principles set for the first time an evaluative framework for

a review of the NIS, its remit and operations.

2. Data protection

31. Kenya does not currently have specific data protection legislation. However, a Data Protection Bill 2013[36] has been forwarded to the Attorney General for publication and the Cabinet Secretary for Information Communication and Technology announced the Bill was expected to be presented in Parliament by the end of May 2014.

32. Once law, the Bill will give effect to Article 31(c) of the Constitution, which outlines the right of every person not *to have "information relating to their family or private affairs unnecessarily required or revealed" and* Article 31(d), the right not to have " *the privacy of their communications infringed".* It will also regulate the collection, retrieval, processing, storing, use and disclosure of personal data. However the proposed legislation fails to explicitly address the protection of data stored in the "cloud" (synchronised storage centres for digital data), which is a particular concern in the case of storage in cloud repository servers outside Kenya, raising issues of jurisdiction in cases of violations.[37]

33. Once adopted, existing practices will need to be addressed and reviewed to meet the standards set by the new Act.

Current issues of concern in the area of data protection include:

- **The Integrated Population Registration System and new biometrics database**

34. In December 2012, EDAPS[38] completed the creation of an Integrated Population Registration System (IPRS) for the Kenyan government. The IPRS collects data from a dozen databases held by various government agencies. It combines data from the birth and death register, citizenship register, ID card register, aliens register, passport register and the marriage and divorce register as well as elections register, tax register, drivers register, National Social Security Fund (NSSF) register,

---

assessing surveillance practices in the context of international human rights law. Please refer to the www.necessaryandproportionate.org website for further details.

[36] Available at: http://www.cickenya.org/index.php/legislation/item/174-the-data-protection-bill-2012#.U3sfr1hdU01

[37] Kenya Human Rights Commission, *The Internet Legislative and Policy Environment In Kenya*, January 2014, pp. 35. Available at: http://www.khrc.or.ke/resources/publications/doc_details/67-the-internet-legislative-and-policy-environment-in-kenya.html

[38] Ukrainian company. Further information, available at: http://www.edaps.com/en/news/n1961

National Hospital Insurance Fund (NHIF) register and the Kenya National Bureau of Statistics (KNBS) register. When it was deployed, Kenya had yet to adopt data protection legislation and the collection, centralisation and sharing of this data is not appropriately regulated.

35. In April 2014, the Kenyan government announced that it would be registering all Kenyans in a new national digital database that would include biometric details as well as information on land ownership, establishments and assets. The aim of the programme is to facilitate the identification of people holding forged or false identification documents.

36. The use of biometric technology raises specific privacy concerns. As outlined in a briefing[39] published by Privacy International, the very nature of biometric technologies can lead to several problems:
    - The data processed is at risk of being misused and is subject to fraud;
    - The system can produce misidentification and inaccuracies;
    - Its nature renders it exclusionary, given that the universality of the technology itself is yet to be proven with failures to process, for example, the fingerprints of manual labourers and individuals with darker skin;
    - The unregulated retention of biometric data raises the possibility of "function creep" (use of the data for purposes other than those for which it was collected) and insecure data storage. The mere existence of biometric data could lead to the development of new justifications for its use beyond the original purposes for which the data subject gave consent, and the general storage of data renders it vulnerable to theft.

37. While recognising that biometric technology is not harmful per se, it must be regulated and data collected only for limited, specific purposes. Without appropriate safeguards, biometric data can be used as a tool for surveillance through profiling, data mining and big data analysis. The use of biometric technology in the 2012 Kenya elections illustrated that the functionality of biometric systems is not always reliable and resulted in the need to resort to manual methods.[40]

➢ Registration of mobile telephony users

38. In 2010, the CCK announced that mobile phone subscribers would be required to register their details with operators or risk

[39] Privacy International (2013) *Biometrics: Friend or foe of privacy?* Available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/biometrics_friend_or_foe.pdf
[40] Ibid, pp. 3-4

having their Subscriber Identity Module (SIM) cards deactivated. Subscribers have been obliged to provide the following personal information in order to register their SIM cards: full names, physical and postal addresses, dates of birth, and alternative contacts. When a minor is registered, the child's guardian must produce an identification card.[41]

39. The Kenya Information and Communications (Amendment) Act 2013 integrated some requirements already included in the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2012. These include:

- Section 27C (2) states that *"A subscriber shall be prima facie liable for activities or transactions carried out using a SIM-card, registered under the subscriber's name"*. Given the high proportion of individuals who share SIM-cards in Kenya, as in much of Africa, this provision raises concerns over misidentification. Although section 27C (3) provides the opportunity for the subscriber to prove he or she was not in control of the SIM-card at the time of its misuse, this places a heavy burden of proof on the misidentified subscriber.

- Section 27C (4) imposes a fine (< KES 100,000/USD 1,150) and/or imprisonment (less than six months) for subscribers who fail to register their SIM-cards or provide false information upon registration.

- Section 27 D gives the Communications Authority[42] the power to make regulations with respect to various key thematic provisions of the Act including: *(a) procedure for SIM-card registration; (b) timelines for SIM-card registration, storage and retention of subscriber records; (c) confidentiality and disclosure of subscriber information; (d) registration of minors; (e) transfer of SIM-cards; (f) registration particulars; (g) suspension and deactivation of SIM-cards; and (h) any other matter that may be prescribed under this sub-Part.*

- There is concern over the independence of the Communication Authority from the government given that members of the Commission are not elected representatives but are appointed by either the President (in the case of the Chairman) or the Minister for the Secretary-General (for the other members).

40. On 7 February 2014, the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services)

[41] 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

[42] The Communications Authority of Kenya, established by Section 3 which amended Section 2 (2) of the 1998 Act, by replacing the Communications Commission of Kenya

Regulations 2014[43] were published. These include the following provisions:

- Section 13 states, *"A licensee shall grant the Commission's officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations."* The CCK has argued that their request to access personal information is in line with Article 35 of the Constitution that permits citizens the right to access information held by the State or by another person and is required for the exercise and protection of any rights or fundamental freedom. However, the Kenya High Court ruled that a company or agency is not a "natural person" and so could not enjoy the rights upheld by Article 35.[44]

- Section 14 imposes higher penalties than the Amended Act for any person who contravenes the Regulation by imposing *"a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or to both for each contravention."*

- Section 8 (1) requires that when registering, a minor must present an identification document in accordance with Section 5 (1) (i), Whereas previously a student identity card could serve as an identification document, the law now requires the minor to present an original and true copy of his or her birth certificate.

41. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups. It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities. Given that CSOs and networks of HRDs increasingly utilise SMS service to share information and mobilise, the security of the system must be guaranteed to protect their right to privacy and the rights to freedom of expression and association.

➢ Communications monitoring

42. The Information and Communications (Amended) Act 2013 and related Regulations as well as the Prevention of Terrorism Act 2012 illustrate the overarching powers government authorities

[43] Legal Notice No. 10 to the Kenyan Communications and Information Act, 7 February 2014. Available at: http://kenyalaw.org/kl/index.php?id=4215
[44] Famy Care Limited v. Public Procurement Administrative Review Board & 5 others [2013] eKLR, paragraph 26

have to monitor individuals' communications and access their personal data.

43. CSOs and other human rights bodies have regularly alerted Kenyan authorities and the international community to the situation faced by HRDs and journalists in Kenya. The focus on this issue in the last UPR review of Kenya in 2010 confirms that although this is not a new issue, it remains one that requires attention as the Kenyan authorities have failed to take the necessary steps to address the situation.

44. In 2012, in an assessment it carried in Kenya, Peace Brigades International stated, in relation to HRDs, *"incidences of surveillance by state and non-state actors have been reported. Offices have been raided or burgled and computers hacked, and several organisations suspected that their phones were being tapped."*[45] In October 2013, Human Rights Watch[46] warned of the rising attacks on HRDs. Regular reports by the East and Horn of Africa Human Rights Defenders Project (EHAHRDP)[47] and Front Line Defenders[48] of HRDs and journalists being intimidated, attached, arrested, tortured, killed, and kidnapped in Kenya demonstrate the significance of the issue.

45. These trends combined raise serious concerns about the potential use of surveillance activities by the government to further clamp down on civil society and HRDs, especially in the context of the war on terror, which the government has seized on as a legitimizing narrative for serious human rights violations.

- **Social protection programmes**

46. Cash Transfers are an increasingly popular aspect of social protection programmes across the developing world, including in Kenya. While there are considerable benefits that can be derived from integrating new technologies into the delivery of social protection, the use of cash transfers pose a number of risks to beneficiaries' right to privacy. Extensive and sensitive information is collected, analysed and disseminated, often in the absence of appropriate regulation to ensure data protection principles are adhered to.[49] Research[50]

[45] Peace Brigade International, *An assessment of the feasibility and effectiveness of protective accompaniment in Kenya, External Report*, July 2012, pp. 7. Available at: http://www.peacebrigades.org.uk/fileadmin/user_files/international/files/special_report/PBI_Kenya_report.pdf

[46] Human Rights Watch, *Kenya: Rights Defenders Under Attack*, 4 October 2013. Available at: http://www.hrw.org/news/2013/10/04/kenya-rights-defenders-under-attack

[47] More information available at: http://www.defenddefenders.org/country-profiles/kenya/

[48] More information available at: http://www.frontlinedefenders.org/kenya

[49] Hosein, G. and Nyst, C. (2013) *Aiding Surveillance*, Privacy International. Available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/aiding_surveillance.pdf

[50] African Platform for Social Protection (2014) *The management of the privacy of personal information in Older Persons Cash Transfer (OPCT) programme in Kenya*

carried out by the African Platform for Social Protection on the Older Persons' Cash Transfer programme, a government-funded programme presented as a positive case study on good practice and policy for cash transfers to vulnerable groups, has shown there is a clear trade off between privacy and the enjoyment of social security and services. This research also revealed that beneficiaries of such programmes have little or no awareness of why their data is being collected, what it will be used for, and by whom. Further, the research indicates beneficiaries trust government to use their data appropriately and protect the data from unauthorised third parties. Despite guidelines regulating some cash transfer programmes, the lack of data protection legislation in Kenya raises the possibility that the right of beneficiaries to control their personal data and who has access to it is not being respected.

(4) Adoption of new media laws

47. On 5 December 2013, Kenya adopted two new laws regulating the media: The Kenya Information Communication (Amendment) Act 2013 (KICA Act) establishes the Communication and Multimedia Appeals Tribunal, and the Media Council Act 2013 establishes the Media Council of Kenya. In January 2014, Kenyan journalists' associations and media houses filed a case against the Kenyan government arguing that the new media laws were a violation of Article 34 of the Constitution, which guarantees the media sector protection from government influence as new statues would limit media freedom and freedom of expression.[51] And in response, on 31 January 2014, The High Court issued an order halting the implementation of the Media Council Act 2013 and the KICA Act until the full Court has considered and issued a ruling in the case filed by the Kenya Media.[52]

48. CSOs have raised concerns regarding aspects of these laws, which would negatively impact freedom of the media and freedom of expression. Concerns include: State power to control broadcasting regulations by giving them the power to appoint the Communication authority responsible for regulating the broadcast and telecommunications sector, punitive penalties for media outlets and journalists for breaching the KICA Act, the unnecessary imposition of strict educational standards for the national journalist qualification process, and a provision

[51] Mangera D., *Kenyan media prepare to battle new press laws*, 27 January 2014, Index for Censorship. Available at: http://www.indexoncensorship.org/2014/01/kenyan-journalists-prepare-battle-new-press-laws/

[52] Freedom House, *Kenyan Journalists Win Court Victory against New Restrictions*, 4 February 2014. Available at: http://www.freedomhouse.org/article/kenyan-journalists-win-court-victory-against-new-restrictions#.U33aUNyVh8c

permitting legislators to revise and integrate within the law the existing Journalist Code of Conduct.[53]

(5) Attack on survival of civil society

49. Recent years have seen a worrying attempt from the Kenyan government to limit, regulate and monitor the activities of civil society. CSOs and HRDs have been vilified through politically motivated public campaigns against them that have sought to portray them as traitors and Western agents. For example, in September 2013, Maina Kiai, the former head of the Kenyan National Commission for Human Rights and a UN special rapporteur on the rights to freedom of peaceful assembly and of association, and Gladwell Otieno, the director of AFRICOG, received threats because of their support to the International Criminal Court's actions against Kenya's President and the Vice-President for their role in the violence outbreak following the December 2007 elections. Most recently, the war on terror has seen a renewed attempt to vilify HRDs and civil society as terror sympathisers and radicalise public opinion against them, putting them at[54] higher risk of persecution.

50. Attempts to portray CSOs and HRDs as foreign agents and enemies of Kenya have now taken a step further. The government has made efforts to institutionalise the clampdown on civil society through repressive legislation. In October 2013 the government tabled a series of amendments to the Public Benefits Organisation (PBO) Act. If passed into law, these amendments would negatively impact civil society by increasing governmental control over civil society, including unwarranted intrusion into their affairs and wide discretion in registration processes, as well as precluding any CSO from receiving foreign funding that amounts to more than 15 per cent of its total budget[55]

Recommendations

We recommend that the government of Kenya:

51. Ensure that the Data Protection Bill, if passed into law, will protect the right to privacy of citizens in accordance with international human rights law;

---

[53] Article 19, *Kenya: New laws mark major setback for media freedom, Press release*, 16 December 2014. Available at: http://www.article19.org/resources.php/resource/37407/en/kenya:-new-laws-mark-major-setback-for-media-freedom

[54] Refworld, *World Report 2014: Kenya*, 21 January 2014. Available at: http://www.refworld.org/docid/52dfddd043.html

[55] Article 19, *Kenya: Vote against amendments a win for human rights and civil society*, 6 December 20143. Available at: http://www.article19.org/resources.php/resource/37386/en/kenya:-vote-against-amendments-a-win-for-human-rights-and-civil-society

52. Ensure that government authorities expand existing protections for the right to privacy and data protection in relevant national laws to guarantee respect for these rights in the context of digital communication;

53. Introduce safeguards to ensure that the rights of mobile telephony subscribers in relation to their personal data are guaranteed;

54. Revoke the Regulations adopted under the 2009 Information and Communications Act which unlawfully limit the right to privacy;

55. Appoint an independent authority to investigate communications monitoring and surveillance programmes conducted by the Kenyan government and ensure that these practices respect the government's national and international obligations to protect the privacy of its citizens and their personal data;

56. Investigate the recent revelations of the NSA-run programme called MYSTIC and take the necessary steps to ensure the protection of Kenya citizens' privacy and their mobile phone communications;

57. Take steps to assess communication surveillance national policies and practices with a view to complying with the *International Principles on the Application of Human Rights to Communications Surveillance*.

58. Ensure that the state surveillance of online and offline activities is lawful and does not infringe on human rights defenders' right to freedom of expression and ability to defend human rights, including through use of the information communication technologies.

59. Ensure that the proposed amendments to the 2013 Public Benefits Organisation Act are not passed into law, in order to ensure an autonomous, diverse, open and free civil society.