PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
35th Session - Kenya

The Right to Privacy in Kenya

Submitted by the National Coalition of Human Rights Defenders-Kenya, KELIN, Paradigm Initiative, Privacy International

July 2019

INTRODUCTION

1. This stakeholder report is a submission by **Privacy International (PI)**, the **National Coalition of Human Rights Defenders Kenya (NCHRD-K), The Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN)**, and **Paradigm Initiative**. **PI** is non-profit, non-governmental organisation that promotes and defends privacy as a human right that supports and enables other human rights and fundamental freedoms; monitors and reports on surveillance methods and tactics employed against people and groups; and advocates for strong national, regional and international laws to protect people and safeguard against data exploitation and abuse. **NCHRD-K** is a non-governmental organisation that promotes the safety and protection of human rights defenders (HRDs)[1] in Kenya. NCHRD-K was established to strengthen the work of HRDs[2] in Kenya by reducing their vulnerability to the risk of persecution and by enhancing their capacity to effectively defend human rights through capacity building, advocacy and protection. **KELIN** is an independent Kenyan Civil Society Organization working to protect and promote health related human rights in Kenya by advocating for integration of human rights principles in laws, policies and administrative frameworks; facilitating access to justice in respect to violations of health-related rights; training professionals and communities on rights-based approaches and initiating and participating in strategic partnerships to realize the right to health nationally, regionally and globally. **Paradigm Initiative (PI)** is a non-profit social enterprise that builds ICT-enabled support systems for young people and advocates digital rights, in order to improve livelihoods. Paradigm Initiative's digital inclusion program involves working closely with underserved communities and youth to provide access to web-enabled technologies, digital skills training, entrepreneurship and life-skills, online work, connection to short-term internships, and supporting youth to pursue

1 See, e.g., Human Rights Defenders: Protecting the Right to Defend Human Rights, Fact Sheet No. 29, Office of the United Nations High Commissioner for Human Rights, https://www.ohchr.org/Documents/Publications/FactSheet29en.pdf (describing the roles and activities of HRDs, the threats they face, and affirmative obligations of states to ensure protections and full guarantee of rights of HRDs).

2 See, e.g., UN Declaration on Human Rights Defenders, Resolution A/RES/53/144 (Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms

their entrepreneurial dreams. Its digital rights advocacy program is focused on the development of public policy for internet freedom. Through its programs and its people, Paradigm Initiative connects communities with socio-economic opportunities that ICTs provide.

2. PI, NCHRD-K, KELIN, and Paradigm Initiative wish to bring their concerns about the protection and promotion of the right to privacy, and other rights and freedoms that privacy supports, for consideration in Kenya's upcoming review at the 35th session of the Working Group on the Universal Periodic Review.

The right to privacy

3. Privacy is a fundamental human right.[3] The right to privacy supports other fundamental rights and freedoms,[4] including the right to equal participation in political and public affairs, and the freedoms of opinion, expression, religion, peaceful assembly, and association.

4. The U.N. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has recognized that, "[i]n addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed."[5] Furthermore, privacy is critical for the development and expression of other rights: "[p]rivacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively."[6]

5. The U.N. Special Rapporteur for freedom of expression has explained "[t]he right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression" because "[s]tates cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy."[7]

6. Violations of the right to privacy can infringe peoples' freedoms to formulate and express ideas, freely communicate, associate with others, organise to

3 See, e.g., Universal Declaration of Human Rights Article 12; United Nations Convention on Migrant Workers Article 14; U.N. Convention of the Protection of the Child Article 16; International Covenant on Civil and Political Rights Article 17; Article 10 of the African Charter on the Rights and Welfare of the Child; Article 4 of the African Union Principles on Freedom of Expression.

4 See, e.g., U.N. General Assembly, The Right to Privacy in the Digital Age, U.N. Doc. No. A/RES/73/179, 21 Jan. 2019, p. 2, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179 ("recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society").

5 Martin Sheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, U.N. Doc. No. A/HRC/13/37, 28 Dec. 2009, p. 13, para. 33, available from https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/a-hrc-13-37.pdf.

6 Id. at pg. 13, para. 33.

7 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/23/40, 17 Apr. 2013, pgs. 7, 20, paras. 24, 79, https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

petition the government for change, or practice their religion, and can undermine the ability of the press and possible whistle-blowers to hold those in power accountable without fear of retaliation.

7. The U.N Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance has noted that "security measures taken by some Governments in the context of countering terrorism may contribute to fuelling racism, xenophobia, and discrimination against certain persons or groups owing to their ethnic origin, religion or migration status,"[8] and specifically expressed concern at the situation in Kenya, where, "[i]n response to a spate of terrorist attacks, the Government launched an operation to increase the policing of ethnic minorities and Muslim communities."[9]

Follow up to the previous UPR

8. In Kenya's previous review, the right to privacy was not explicitly addressed in the National Report submitted by Kenya or in the report of the Working Group, but both reports explicitly addressed other rights and freedoms that privacy supports and enables. In its National Report, Kenya "committed to implementing its domestic and international obligations arising from human rights treaties that it has ratified," and noted its appreciation for "the role played by human rights defenders and civil society organisations in the country." The Working Group recommended that Kenya ensure full respect for human rights, including freedom of expression, press, associations, peaceful assembly, and protections for HRDs.[10]

---

8 Report of the Special Rapporteur on contemporary forms of racial, racial discrimination, xenophobia and related intolerance, U.N. Doc. No. A/HRC/38/52, Apr. 25, 2018, pg. 1, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/52.

9 Id. at pg. 13, para. 59.

10 For example, some of the recommendations included the following:

- Ensure that human rights and fundamental freedoms enshrined in its Constitution are protected in the fight against terrorism and the national security plan and actions; pay particular attention to safeguarding the rights and safety of minorities and marginalized groups, as well as human rights defenders, refugees and stateless persons . . . (Finland) – Recommendation 142.17;
- Redouble efforts to eliminate extra-judicial killings and acts of violence and torture, and to educate military and police personnel on human rights principles (Holy See) – Recommendation 142.75;
- Ensure full respect for human rights by law enforcement agencies and ensure that violations are subjected to judicial prosecutions (France) – Recommendation 142.106;
- Take all the necessary measures to bring to an end attacks on journalists and ensure that the Information and Communication Act is in line with the human rights obligations of Kenya, in particular press freedom (Switzerland) – Recommendation 142.126;
- Guarantee freedom of expression, press, associations and peaceful assembly of journalists, activists and participants in demonstrations (Uruguay) – Recommendation 142.129;
- Take measures to address all allegations of abuse or intimidation against human rights defenders by the security forces, and integrate human rights education into police training programmes (Botswana) – Recommendation 142.132;
- Repeal or amend any laws that may constrain or limit a vibrant civil society, in line with international human rights obligations and the Constitution of Kenya (Canada) – Recommendation 142.133;
- Create and maintain, in law and in practice, a safe and enabling environment in which human rights defenders and civil society can operate free from hindrance and insecurity, in accordance with Human Rights Council resolutions 22/6 and 27/31 (Ireland) – Recommendation 142.137;
- Ensure, in both legislation and its implementation, freedom of expression and freedom of the press as guaranteed in its Constitution (Japan) – Recommendation 142.138;
- Ensure that all counter-terrorism measures undertaken fully comply with the Constitution, the rule of law and international human rights obligations (Canada) – Recommendation 142.186.

9. In their UPR midterm report, Kenyan civil society organisations raised numerous concerns associated with failures to implement recommendations from the previous review, including but not limited to: failures by the police and military agencies to comply with human rights,[11] high rates of extrajudicial killings with minimal investigation or prosecution,[12] harassment and intimidation against HRDs,[13] online and phone surveillance of journalists,[14] unlawful management of protests,[15] and failure to guarantee freedom of association and assembly.[16]

International obligations related to privacy

10. Kenya has signed the **Universal Declaration of Human Rights (UDHR)**[17] and has ratified the **International Covenant on Civil and Political Rights (ICCPR)**,[18] both of which uphold the right to privacy and the right to protection against interferences with the right to privacy.

11. The **Human Rights Committee** has noted that state parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against [arbitrary or unlawful interferences with the right to privacy]," regardless of "whether they emanate from State authorities or from natural or legal persons," and to protect the right to privacy itself.[19]

Domestic laws related to privacy

12. The **Constitution of Kenya** protects the right to privacy by enshrining international law in domestic law and explicitly protecting privacy as a fundamental right. Article 2 § 5 provides that "general rules of international law shall form part of the law of Kenya," and Article 2 § 6 provides "[a]ny treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution," which includes the UDHR and the ICCPR. Article 31 provides "[e]very 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."

---

11 The Kenyan UPR Stakeholders' Coalition, Kenya's 2nd Cycle Universal Periodic Review Mid Term Report, January 21, 2019, 29-30, https://www.khrc.or.ke/mobile-publications/shrinking-civic-space/192-kenya-s-2nd-cycle-universal-periodic-review-mid-term-report.html?path=shrinking-civic-space.

12 Id. at 29-30.

13 Id. at 32.

14 Id. at 36.

15 Id. at 37.

16 Id. at 36-37.

17 Article 12 of the UDHR provides, "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

18 Article 17 of the ICCPR provides, "[n]o one shall be subjected to arbitrary of unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and that "[e]veryone has the right to the protection of the law against such interference or attacks."

19 General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (1988), para 1.

13. The **Kenya Information and Communications Act, 1998 (subsequently amended)** prohibits the interception and disclosure of communications. Article 31 penalises the unlawful interception and disclosure of communications by telecommunication providers.[20] Section 83W criminalises unauthorized access to, and interception of, a computer service by an individual to "secure access to any computer system for the purpose of obtaining, directly or indirectly, any computer service," or to "intercept or cause to be intercepted, directly or indirectly, any function of, or any data within a computer system."[21]

14. The **Kenya Information and Communications (Consumer Protection) Regulations (2010)** protect subscribers from interception of their communications. Section 15(1) provides, "[s]ubject 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."[22]

15. Despite the domestic protections outlined above, the Kenyan government has passed legislation to expand the interception powers of intelligence and law enforcement agencies in ways that could lead to unlawful interference with the right to privacy.

16. The **National Intelligence Service (NIS) Act (2012)** limits the right to privacy and allows the NIS to investigate, monitor or interfere with the communications of people under investigation by the NIS or suspected of committing of an offense.[23] The NIS is meant to be subjected by parliamentary oversight, presumably by the Intelligence and Security Committee, although this is not clear based on the wording of the NIS Act. The Act establishes an Intelligence Service Complaints Board, but the Board is limited to making recommendations to the President or Cabinet Secretary.[24] Further, very little information is publicly available about the Board and its investigations, if it has engaged in any. An investigation by Privacy International suggests "[i]n practice, the NIS is an agency that is almost entirely opaque even to the senior agents of other security organs with whom the NIS is mandated to work. These security organs are, to a large degree, dependent on the NIS to carry out communications surveillance. This

20 Kenya Information and Communications Act, 1998, Section 31.

21 Kenya Information and Communications Act, 1998, Section 83W.

22 Kenya Information and Communications (Consumer Protection) Regulations, 2010, Section 15(1).

23 See National Intelligence Service Act, 2012, Section 36 ("(1) The right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person who is subject to investigation by the Service or 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. (2) The Service shall, prior to taking any action under this section, obtain a warrant under Part V."); See also and National Intelligence Service Act, 2012, Section 42(3) (a written authorisation from the Director General of the NIS, to allow the NIS to investigate or respond to a threat to national security, "may authorize any member of the Service to obtain any information, material, record, document or thing and for that purpose —(i) enter any place or obtain access to anything; (ii) search for or remove or return, examine, take extracts from, make copies of or record in any manner the information, material, record, documents or thing; (iii) monitor communication;
(iv) install, maintain or remove anything; or (v) take all necessary action, within the law, to preserve national security," and such a written authorisation must also be accompanied by a warrant when it includes monitoring communication.)

24 See National Intelligence Service Act, 2012, Sections 66-67.

effectively renders meaningless whatever legal requirements or operating procedures that do exist that would require an agent to obtain an interception warrant, or follow another accountability process."[25]

17. The **Prevention of Terrorism Act (2012)** allows the government to limit the right to privacy through surveillance: for example, "[t]he limitation of a fundamental right and freedom . . . shall relate to (a) the right to privacy to the extent of allowing . . . (iii) the privacy of a person's communication to be investigated, intercepted or otherwise interfered with."[26]

18. The **Security Laws (Amendment) Act (2014)** allows for "the right to privacy . . . [to] be limited . . . for the purpose of intercepting communication directly relevant in the detecting, deterring, and disrupting [sic] terrorism."[27] This Act entrusted the executive to issue regulations to govern interception of communications. This Act also introduced a new amendment to the Prevention of Terrorism Act: a Cabinet Secretary was tasked with making new regulations to govern communications interception by the "national security organs" when related to terrorism investigations. The "national security organs" are defined widely in Article 239 of the Constitution as the Kenya Defense Forces, National Intelligence Service (NIS), and the Kenya Police Service. It is unclear if these rules, which have yet to be articulated, would still require the National Security Organs to obtain warrants to intercept communications, as set out in previous laws."[28]

19. The **Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations (2013)** require that each telecommunication provider give the **Kenyan Communications Authority (CA)** access to "its systems, premises, facilities, files, records and other data" for inspection.[29]

20. The **Kenya Information and Communications (Amendment) Act (2013)** requires that telecommunication providers register a person's full name, identity card number, date of birth, gender, and physical and postal addresses before selling a SIM card or other telecommunication services to that person, and provides that such information may be disclosed to the government for the purposes of investigating any criminal offense.[30]

21. The **Kenya Information and Communications (Registration of SIM-Cards) Regulations (2015)** requires telecommunication providers to transmit SIM-card registration information to the CA.[31]

25 Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," March 2017, at 25, available from: https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya.

26 Prevention of Terrorism Act, 2012, Section 35.

27 Security Laws (Amendment) Act, 2014, Section 69.

28 Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," supra, at 13.

29 The Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations, 2013, Regulation 13.

30 Kenya Information and Communications (Amendment) Act, 2013, Section 12.

31 Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015, Regulation 3.

22. The **Computer Misuse and Cybercrimes Act (2018)** provides the government sweeping powers to prosecute vaguely formulated and broadly defined crimes related to computers, and to search computers including by ordering people to decrypt encrypted data. For example, the Act creates content-related offenses for communications that are false[32] or "detrimentally affects"[33] a person, which could give the government unbridled discretion in monitoring communications and prosecuting certain people for certain types of communications, such as government whistle blowers or other individuals acting in the public interest. Civil society organisations contested 26 sections of the Computer Misuse and Cybercrimes Act on the ground that they were contrary to the right to freedom of expression.[34] Those sections were suspended pending the full hearing and determination of the case.

AREAS OF CONCERN

A. Monitoring and Surveillance of Communications

23. Over the years, there have been on-going reports of the expansive monitoring and surveillance practices and as well as capabilities of the Kenya government and its security and intelligence agencies. In March 2017, a report by Privacy International documented how the information acquired from unlawful communications surveillance is justified by the state as a response to counterterrorism - from surveilling, profiling, locating, tracking and arresting targets to abuse, torture, abduction and extrajudicial killing.[35] Furthermore, "[i]nformation obtained through communications surveillance is central to the identification, pursuit, and 'neutralisation', or killing, of suspects – a process in which Kenyan citizens' fundamental human rights are seriously abused."[36]

24. Under article 17 of the ICCPR, as interpreted by the Human Rights Committee, any interference with someone's privacy must be in accordance with the law, necessary and proportionate to achieve a legitimate aim. The laws must be "(a) publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures

32 Computer Misuse and Cybercrimes Act, No 5 of 2018, Section 12.

33 Computer Misuse and Cybercrimes Act, No 5 of 2018, Section 16.

34 See Bloggers Association of Kenya (BAKE) v Attorney General & 5 others [2018] eKLR, available from http://kenyalaw.org/caselaw/cases/view/159286/. Of particular concern to privacy are the enhanced investigative procedures in Part V of the Act namely: search and seizure of stored computer data (Section 48), record of and access to seized data (Section 49), production order(Section 50), expedited preservation and partial disclosure of traffic data (Section 51), real-time collection of traffic data (Section 52), interception of content data (Section 53).

35 See generally, Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," March 2017. Available from: https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya.

36 Id. at 25.

for the use and storage of the data collected; and (d) provide for effective safeguards against abuse."[37]

25. A key safeguard against arbitrary interference with someone's privacy is an effective, independent mechanism of prior authorisation of surveillance measures. International and regional experts and courts have increasingly found that prior judicial authorisation should be required. In Kenya, research has found NIS interception (of both content and metadata) is conducted without a judicial (or other independent) authorisation, partly thanks to the ambiguity of the law governing interception by the NIS.[38] The lack of clarity on the applicable laws leads to a practice of interception without prior judicial or other independent authorization by the NIS in Kenya.

26. An investigation by Privacy International found a revolving door policy, whereby "the NIS often tips off the police based on information gleaned from its own communications monitoring, the police then obtain the necessary clearance to re-surveil the same target to produce evidence admissible in court, according to prosecution and defence attorneys and police investigators."[39]

Direct Access

27. Direct access is "where state agencies have a direct connection to telecommunications networks which allows them to obtain digital communications content and data (mobile and/or internet), without prior notice or judicial authorisation and without the involvement of the telecommunications provider or internet service provider that owns or runs the network."[40] Direct access is concerning because it "has a defined link to arbitrary and abusive practices that impact freedom of expression and privacy."[41]

28. The Kenyan National Intelligence Service (NIS) has direct access to telecommunications networks across the country, which allows it to intercept communications—including the content of the communications as well as information about who sent and received the messages, from what devices, at what times, and from what locations—without the knowledge or consent of telecommunications providers or their subscribers.[42] Officially, law enforcement requests for data to Safaricom require a letter of justification, written by an investigating officer, signed by his or her superior, and provided in hard copy or emailed to the telecommunication operator. But agents routinely circumvent protocol in urgent cases, and given the presence of NIS

37 U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, pg. 10, para. 18, available from: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A-HRC-27-37_en.doc.

38 Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," March 2017. Available from: https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya.

39 Id. at 16.

40 Id. at 19-20.

41 Id. at 20.

42 Id. at 19-20.

officers undercover in telecommunication network operators, there is a concerning lack of safeguards and oversight to prevent abuse. [43] The NIS is technologically capable of accessing information that can paint a detailed profile of peoples' activities, views, religious beliefs, sexual orientation, and relationships with others, and the NIS could then share this information with local police.

29. The U.N. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has emphasized that states' "bulk access to communications and content data without prior suspicion . . . amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification,"[44] and that "mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use . . . [or] mean that it is either reasonable or lawful."[45]

30. In 2015, the European Court of Human Rights warned that direct access systems are vulnerable to abuse.[46] It stated in the case of *Roman Zakharov v. Russia* that "a system . . . which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorization to the communications service provider or to anyone else, is particularly prone to abuse."[47]

Packet Interception

31. Middleboxes are a type of software tool which enables 'deep packet inspection' to examine the content of a data packets being sent over the Internet which enables networks to examine the origin, destination as well the content of data packets (header and payload). This means that the government is technologically capable of inspecting, logging, and re-routing data sent over computer networks.

32. In January 2013, The Citizen Lab of the University of Toronto published a research brief in which it reported that researchers had discovered Blue Coat PacketShaper installations in countries including Kenya.[48] Technologies from US-based Blue Coat allow for the the surveillance and monitoring of interactions on applications including Facebook, Gmail, Skype and Twitter, among others. It is unclear whether Blue Coat

43 Id. at 19-20.

44 Ben Emmerson, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, U.N. Doc. A/69/397, 23 Sept. 2014, pg. 4, paras. 8-9, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.

45 Id. At 5, para 11.

46 Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," supra.

47 European Court of Human Rights, Roman Zakharov v. Russia judgement (4 December 2015) para 270. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-142532%22]}.

48 CitizenLab, Planet Blue Coat Mapping Global Censorship and Surveillance Tools, 15 January 2013 available from: https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

PacketShaper installations were in place in Kenya.

33. In 2017, an investigation by the Centre for Intellectual Property and Information Technology Law (CIPIT) revealed that Safaricom, Kenya's largest telecommunications provider,[49] had a middle-box installed on its cellular network,[50] which may or may not have since been withdrawn.[51] While such middle-boxes can be used for legitimate purposes such as certain minimum level of quality of service and to protect the network from transmitting malicious programs, they can also be used to manipulate, surveil, and censor Internet traffic.

Internet and Social Media Monitoring

34. The government "periodically polices the internet for content that is perceived to be morally objectionable," and "has increasingly sought to have content removed online" and from social media profiles.[52] For example, a Kenyan blogger was arrested for posting photos of the Kenyatta family in a Nairobi hospital, and the photos were removed from his Facebook page, although it was unclear who removed them.[53]

35. The use of social media monitoring, the techniques and technologies that allow companies or governments to monitor social media networking sites (SNSs),[54] creates potential for misuse by the government in identifying and targeting certain people and groups in society including HRDs and journalists.

36. There is also particular concern for Lesbian, Gay, Bisexual, Transgender, or Queer (LGBTQ) people as Kenya provides a hostile environmental for people who are LGBTQ: the Kenyan penal code criminalises same-sex relationships, and Kenya's High Court recently rejected a challenge to such laws, in a setback for LGBTQ rights activists in Kenya.[55] It is concerning that social media monitoring could be used to force users to remove content deemed to promote homosexuality or other non-heterosexual relations. The movie, "Rafiki," was banned from the Internet and television in 2018 because it allegedly promoted homosexuality "in violation of 'moral values.'"[56]

Mobile Interception and Device Management

37. The government has attempted to obtain mobile phone subscribers' data in violation of their right to privacy.

---

49 Freedom House, Freedom on the Net 2018 - Kenya, 1 November 2018, available from https://freedomhouse.org/report/freedom-net/2018/kenya

50 Centre for Intellectual Property and Information Technology Law, Safaricom and Internet Traffic Tampering, March 2017, available from https://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf.

51 Freedom House, supra.

52 Freedom House, supra.

53 Blogger Robert Alai arrested after leaking photos of Kenyattas in hospital, Nairobi News, Nairobi News, 19 August 2017, available from https://nairobinews.nation.co.ke/news/robert-alai-arrested-photos-kenyattas.

54 See explainer by Privacy International available from: https://privacyinternational.org/explainer/55/social-media-intelligence

55 (Kenya) Penal Code, Sections 162, 165.

56 Freedom House, supra.

38. The NIS may have a device that "appears to function like an IMSI catcher. An IMSI catcher is phone monitoring equipment that is able to actively intercept communications 'off-the-air' of surrounding devices. An IMSI [c]atcher performs interception by presenting itself as a base station amongst the mobile network: the station that your phone connects to when it wants to place a call or send a message. The IMSI [c]atcher mimics a base station by entering the network as the most powerful base station available, meaning that all mobile phones operating within the same area connect to the IMSI [c]atcher's base station. Once connected to the IMSI [c]atcher's base station, the [c]atcher has the mobile phone provide [device and mobile subscriber data]. Once these details have been gathered it becomes possible to monitor the operation of the phone: the voice calls taking place, the messages being sent and the location of the phone."[57] There are a lack of specific regulations governing or restricting the use of IMSI catchers.

39. Furthermore, the High Court of Kenya ruled in two cases in 2018, in *Okoiti v. Communications Authority of Kenya*[58] and *Kenya Human Rights Commission v. Communications Authority of Kenya*,[59] that the Communication Authority's (CA) plan to install a system to access mobile phone subscribers' data was unconstitutional and would violate subscribers' right to privacy. The CA intended its system, known as the Device Management System (DMS), to monitor and identify illegal mobile phone devices. The DMS would have enabled the government to monitor peoples' calls, text messages, and transactions through mobile phone payment applications, and therefore to function as a system of surveillance and censorship.

B. Surveillance of HRDs and Journalists

Surveillance of HRDs and Journalists because of the Nature of Their Work

40. There are concerns that HRDs and journalists are continuing to be surveilled by the government because of the nature of the work they do, including because such work can be critical of government, rather than for a valid law enforcement purpose.[60] For example, in a survey of HRDs conducted by NCHRD-K, a "[m]ajority of respondents reported that they have experienced security breaches that include unlawful access to their social media and email accounts as well as phone tapping."[61] According to the UPR Stakeholders' Coalition Midterm Report, "[t]he government has attempted to obstruct critical journalists with . . . online and phone surveillance, and in some cases, physical assaults."[62]

57 Privacy International, "Trace, Capture, Kill: Inside Communication Surveillance and Counterterrorism in Kenya," supra. at 27.

58 Kenya, Okoiti v. Communications Authority of Kenya [2017] eKLR, available from https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/05/KENYA-JUDGMENT-ON-RIGHT-TO-PRIVACY-DEVICE-MANAGEMENT-SYSTEM.pdf.

59 Kenya, Kenya Human Rights Commission v. Communications Authority of Kenya [2017] eKLR, available from https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/05/Judgment-86-of-2017.pdf.

60 The Kenyan UPR Stakeholders' Coalition, Kenya's 2nd Cycle Universal Periodic Review Mid Term Report, supra at 32, 36.

61 National Coalition of Human Rights Defenders – Kenya, A Perception survey on Communication Surveillance and Privacy of Human Rights Defenders in Kenya, at 4, available from https://hrdcoalition.org/perception-survey-on-communication-surveillance-and-privacy-of-human-rights-defenders-in-kenya/.

62 The Kenyan UPR Stakeholders' Coalition, Kenya's 2nd Cycle Universal Periodic Review Mid Term Report, supra at 36.

41. In addition to surveillance specifically targeting HRDs and journalists, the mass surveillance technologies described above function as a sort of panopticon, where HRDs and journalists do not and cannot know whether, when, or why they are under surveillance. This has a chilling effect on HRDs and journalists. The threat of surveillance and the potential risks HRDs and journalists may face as a result restricts the environment in which HRDs and journalists operate.

42. This surveillance can also limit[63] the critical work HRDs and journalists do in ensuring the full ability of people to develop and express opinions and participate fully and equally in society.[64] Because of the chilling environment, HRDs and journalists may feel they are unable to safely communicate with confidential sources. HRDs and journalists may limit work in certain controversial areas that may lead to repercussions from government or other sectors of society. Important stories may go unreported or human rights violations may not be exposed as a result.

43. For example, "[i]n May and August 2018, Human Rights Watch documented incidents of harassment, intimidation, and other abuses against at least 35 [environmental] activists over the past five years. In many cases, activists were arrested or detained in connection with their activism, then released without being charged. Security forces have broken up protests; restricted public meetings; and threatened, arrested, and prosecuted activists on various charges. In at least 15 instances, police accused activists of having links or being sympathetic to Al-Shabab, a Somalia based militant Islamist group. This was especially common between 2013 and 2016, amid increased government surveillance and crackdowns on rights organizations and activists in regions with predominantly Muslim populations."[65]

C. Data Protection

Absence of Data Protection and Privacy Legislation

44. Kenya lacks a clear and robust data protection framework. The proposed Bill was sent to the National Assembly on 3 July 2019.[66] It is essential that the next steps of the legislative process will be open to further consultation from a variety of stakeholders, in particular civil society, to ensure the final law to be adopted complies with the international recognised data protection

63 National Coalition of Human Rights Defenders – Kenya, A Perception survey on Communication Surveillance and Privacy of Human Rights Defenders in Kenya, supra.

64 See, e.g., Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/26/30, 2 July 2014, pgs. 7-8 (Recognizing that the press plays the critical role of a public watchdog, and that to fulfil this vital role the press must be free to comment on issues of public interest without fear of censorship or repercussion); See also David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, 22 May 2015, pg. 20, para. 59, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement ("Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.")

65 Human Rights Watch, Kenya: Harassment of Environmental Activists, December 17, 2018, available from https://www.hrw.org/news/2018/12/17/kenya-harassment-environmental-activists.

66 The Data Protection Bill, 2018, available from http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf.

standards and principles, and sets up clear process for enforcement, transparency and accountability.

45. Until the law is passed, data processing will continue to be undertaken in a legal void. The information collected by public and private entities remains vulnerable to shifting purposes and interests of the parties processing the data.

46. The risks associated with the failure of Kenya to protect the data of persons in Kenya is also illustrated by the use of social media data to develop two targeted and data-driven campaigns during the 2017 elections: "The Real Raila", a virulent attack campaign against presidential hopeful Raila Odinga, and Uhuru for Us, a site showcasing President Uhuru Kenyatta's accomplishments. The online campaigns were developed by a by Harris Media LLC, a far-right American digital media company, on behalf of President Kenyatta's re-election campaign. Harris Media's Real Raila and Uhuru for Us campaigns relied on ad words in Google search and apparently targeted advertising on a range of social media platforms.[67]

47. Furthermore, despite being directed by Section 20 of the HIV Prevention and Control Act, Kenya has failed to implement protect HIV-related data by not prescribing privacy guidelines, including the use of an identifying code, relating to the recording, collecting, storing and security of information, records or forms used in respect of HIV tests and related medical assessments.[68]

D. Identification Schemes

Biometric Registration

48. Biometrics refer to "the physiological and behavioural characteristics of individuals. This could be fingerprints, voice, face, retina and iris patterns, hand geometry, gait or DNA profiles."[69] This type of data is sensitive and unique to an individual. Biometric information is particularly sensitive, as it can be used to identify and track people of the course of their lifetimes, and people cannot change their fingerprints, eyes, or faces.[70]

49. Biometric registration systems are composed of two components: "Firstly, biometric technologies capture and store characteristics in a database in order to *identify* an individual. Secondly, the information in this database is cross-referenced to *verify or authenticate* an individual's identity in a range

67 Privacy International, Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals, 15 December 2017, available from: https://privacyinternational.org/long-read/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack.

68 The HIV Prevention and Control Act, Act no 14 of 2006, National Council of Law Reporting, available from http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/HIVandAIDSPreventionandControlAct_No14of2006.pdf

69 Privacy International, Biometrics, available from: https://privacyinternational.org/topics/biometrics.

70 Dr. Thomas Fisher, Affidavit of Dr. Thomas Fisher of Privacy International, available from https://privacyinternational.org/legal-action/nubian-rights-forum-and-others-v-attorney-general-kenya

of contexts eg. when accessing government services, or crossing borders, to enable an individual to vote, access bank accounts, access health services etc."[71]

50. According to the U.N. High Commissioner for Human Rights, biometric data "is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place."[72]

51. The Kenyan government is increasing its use of biometric databases that allow the government to increase the depth and breadth of information it collects about people, which is particularly concerning given the absence of data protection legislation in Kenya.

52. The promulgation in January 2019 of the Statute Law (Miscellaneous Amendment) Act, 2018 (SLMAA) amended the Registration of Persons Act to enable the government to collect extensive data on Kenyans and registered foreigners in a national database including: land and house reference number, biometric data such fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. The system is called the National Integrated Identity Management System (NIIMS).[73] This system was developed without public consultation or adequate safeguards.[74] There are also concerns that this system could also lead to the exclusion of vulnerable communities, including the Kenyan Nubian and Somali communities.[75] Three petitions were subsequently filed by the Kenya Human Rights Commission (KHRC), Nubian Rights Forum, and the Kenya National Commission on Human Rights (KNHCR) at the Constitutional Court in Nairobi in March 2019 to challenge the constitutionality of this amendment. The petitions, now consolidated, are expected to be heard by the High Court of Kenya in September 2019.

---

71 Id.

72 United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/39/29, 3 Aug. 2018, pg. 5, para. 14, available from https://undocs.org/A/HRC/39/29.

73 Privacy International, Civil society achieves change, but risks still remain in Kenya's new biometric ID system, https://privacyinternational.org/blog/2774/civil-society-achieves-change-risks-still-remain-kenyas-new-biometric-id-system.

74 Id. ("The process of developing the system has been far from the democratic ideal: it was created by a few lines in a Miscellaneous Powers Act, and was not subject to public consultation. This is the unfortunate replication of a lack of democratic processes in the introduction of identity systems that we've seen all over the world. Identity systems, even when they are claimed to be voluntary, are core to systems of control that result in severe interferences with freedom and dignity. The safeguards that must be in place before any identity system is implemented are rarely present, and this is certainly a key concern in Kenya. A data protection act is not a panacea for all the problems with NIMS, but it is a necessary precursor; a data protection bill is making slow progress in Kenya, in stark contrast with speed which this system was approved and deployed.")

75 Maureen Kakah, Nubian group opposes use of new ID system, 22 February 2019, available from: https://www.nation.co.ke/news/Group-opposes-use-of-new-ID-system/1056-4994288-pt4cru/index.html

53. The government is also attempting to transition to biometrically verifying voters.[76] A report by the Centre for Intellectual Property and Information Technology CIPIT at the Strathmore Law School describes the increased use of biometric data in the absence of a proper legislative framework to operationalize the safeguards enshrined in Article 31 of the Constitution. [77]

54. Furthermore, the government has been collecting biometric information regarding people with HIV, including to determine how many people were living with HIV: there are concerns regarding "the risk of function creep in use of biometrics," for example, "with data collected for health purposes being used by police to target key populations for arrest," as well as "the risk of data breaches that could expose stigmatised populations publicly" and result in "discrimination, including in access to government services."[78]

55. There is a lack of public transparency, accountability, public trust,[79] and security regarding these biometric systems.

Compulsory SIM Card Registration

56. In 2010, the Communications Authority (formerly the Communication Commission of Kenya) announced that mobile phone subscribers would be required to register their details with operators or risk having their Subscriber Identity Module (SIM) cards deactivated. The Kenya Information and Communications (Amendment) Act 2013 integrated some requirements, and then in February 2014, the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2014[80] were published.

57. Compulsory SIM card registration denies people their ability to remain anonymous, and to form and communicate ideas in the safety of that anonymity.[81] The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has recognized the importance of encryption and anonymity to the realisation of peoples' rights, and the risks that SIM card registration pose: "[e]ncryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief," and thus "[t]he ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national

76 Dr. Robert Muthuri et al., Biometric Technology, Elections, and Privacy: Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process, The Centre for Intellectual Property and Information Technology Law, https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf.

77 Dr. Robert Muthuri et.al Centre for Intellectual Property and Information Technology Law, 'Biometric Technology Elections and Privacy' Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process available from https://cipit.org/images/downloads/CIPIT-Elections-and-Biometrics-Report.pdf

78 "Everyone said no:" Biometrics, HIV, and Human Rights, a Kenya Case Study, KELIN and the Kenya Key Populations Consortium, http://www.kelinkenya.org/wp-content/uploads/2018/04/%E2%80%9CEveryone-said-no%E2%80%9D.pdf.

79About 20 Million Kenyans boycotted the issuance of Huduma Number by the government: https://www.capitalfm.co.ke/news/2019/05/govt-spokesman-oguna-urges-kenyans-register-for-huduma-namba/

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

81 Privacy International, 101: Sim Card Registration, https://privacyinternational.org/explainer/2654/101-sim-card-registration.

origin or sexuality."[82] Furthermore, "[j]journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment."[83]The Special Rapporteur recognized that SIM card registration policies "directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest."[84] The UNSR recommended that: "States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users."[85]

National Education Management System (NEMIS)

58. The Ministry of Education is compiling information about each Kenyan student, and their parents, in a databased called the National Education Management System (NEMIS). This system could be used to surveil students and parents, but also has harmful repercussions when the system errs.[86]

RECOMMENDATIONS

We recommend the government of Kenya to:

59. Review the legal framework governing surveillance in Kenya to ensure they comply with the International Covenant on Civil and Political Rights, including Article 17 to ensure that any interference with the right to privacy is necessary and proportionate to the aim pursued, notably National Intelligence Service (NIS) Act (2012), Prevention of Terrorism Act (2012), Security Laws (Amendment) Act (2014) and Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations (2013).

60. Revoke mandatory SIM card registration obligation provided for by the Kenya Information Communications (Amendment) Act (2013) and remove the requirements for this information to be provided to the Communications Authority as per the Kenya Information and Communications (Registration of SIM-Cards) Regulations (2015);

61. Reform the Computer Misuse and Cybercrimes Act, 2018 to conform with the Constitution of Kenya and Kenya's human rights obligations to protect the right to freedom of expression and the right to privacy;

82 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, 22 May 2015, pg. 5, para. 12, https://www.ohchr.org/EN/HRBodies/HRC/.../Documents/A.HRC.29.32_AEV.doc.

83 Id. at pg. 5, para. 12.

84 Id. at pg. 18, para. 51.

85 Id. at pg. 18, para. 60.

86 Ouma Wanzala, Teachers reject Nemis, cite identity code error, https://www.nation.co.ke/news/Teachers-reject-Nemis--cite-identity-code-error/1056-5124236-ovaiw8z/.

62. Prohibit the use of deep packet inspection for purposes of surveillance or censorship;

63. Provide for telecommunication operators in Kenya to publish transparency reports to provide information on government requests for interception and for customer data, including communications metadata;

64. Review and reform existing policies and laws and adopt new legislation to ensure an environment for defenders and journalist to work freely and safely without communication surveillance;

65. Conduct prompt and independent investigations into credible reports of unlawful surveillance of human rights defenders and journalists, with the view to bring to justice the perpetrators and provide reparations. Publish the results of these investigations;

66. Adopt a robust data protection law that conforms to the Constitution of Kenya and Kenya's international human rights obligations as well as with the internationally recognised data protection standards. Biometric data should be considered sensitive data that requires higher safeguards. An independent data protection authority should be set-up to oversee the implementation of the law;

67. Take necessary measures to ensure the protection of health and HIV data, for example by requiring the Cabinet Secretary in charge of health to promptly develop and enact Privacy guidelines to safeguard HIV related data as provided for by Section 20 of the HIV Prevention and Control Act.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471