Surveillance Law in Africa: a review of six countries

Kenya country report

Grace Mutung'u

DOI: 10.19088/IDS.2021.059

Introduction

This report provides an overview of the legal basis for government surveillance and protections of citizen privacy in Kenyan law. The report summarises the most relevant pieces of legislation and compares them to existing law in other countries and draft legislation and principles provided by human rights actors. The report focuses particular attention on circumstances in which surveillance is legally permitted, as well as checks and balances detailed in legislation. The final section makes a series of recommendations arising from this analysis for future legislation, legal practice and further research.

Kenya has had a long history of surveillance practices, inspired by the need for social control during the colonial and post-colonial periods, motivated in recent years partly by anti-terrorism, anti-money laundering and public health initiatives. During the colonial period, the government appropriated intelligence systems from various Kenyan communities as part of its colonial conquest. For example, elders would send people pretending to be mad, herders or lost strangers to check out the military strength of other communities or fertility of lands they were interested in (Boinett 2009: 18). Thereafter, the colonial government developed surveillance practices to monitor and counteract dissent. These included fingerprinting of Africans and requirements for movement passes (Breckenridge 2019).

Apart from fingerprinting of the indigenous population, surveillance of persons of interest also dates back to the colonial period. The colonial government in Kenya had an elaborate administrative structure whose duties included gathering intelligence. The police force, established in 1906, also carried out surveillance. Following increased unrest and resistance in the 1920s, a criminal investigations department was established in 1926. One of its duties was to collate data on 'criminals, undesirable and suspicious persons'. It was later mandated to carry out intelligence, and passport and immigration control, as well as fingerprinting. Eventually, a unit known as the 'special branch' was carved out within the department for covert operations and intelligence gathering (Boinett 2009).

At independence, Kenya inherited these surveillance practices. Constitutional changes resulted in a centralised government that maintained colonial administrative structures. The special branch acquired immense power as the intelligence outfit of the central government. It is most infamously remembered for monitoring dissenters in all sectors of society, extrajudicial killings and a disregard for human rights (*ibid.*: 26). The special branch was dismantled and a national intelligence service established under a 1998 law. These experiences informed provisions in the new Constitution of Kenya.

During the constitution-making process at the beginning of the twenty-first century, several constitutional provisions spelling out the powers and limits of national security organs were included. Article 239 of the Constitution defines national security organs as the Kenya Defence Forces (KDF), National Intelligence Service (NIS) and National Police Service (NPS). The organs are supervised by the National Security Council (NCS). A provision on how fundamental rights and freedoms could be limited was also made (Constitution of Kenya 2010, article 24).

Since 2013, Kenya has suffered several terrorist attacks by militant Islamist group Al-Shabaab. The attacks revived the agenda to strengthen the national security apparatus (Lind, Mutahi and Oosterom 2015). In 2014, following several terrorist attacks in northeastern Kenya, the executive sponsored a bill amending various security laws to give national security organs a legal basis for communications surveillance. The surveillance extends to the financial system, where financial institutions closely monitor and report cash flows; and security operations, where law enforcement bodies have wide latitude to investigate suspected crimes and undertake covert operations. Surveillance extends to anti-corruption initiatives; and there are also regulations for mandatory mobile phone SIM card registration and proposals to whitelist all mobile devices, including phones (Republic of Kenya 2015; Communications Authority 2018).

Kenya also has massive data sets that can be used for surveillance purposes. For example, under the Registration of Persons Act, every person is required to register for an identity card on reaching the age of 18. In 2019, the government transformed the register under the Act to a digital identity system known as the National Integrated Identity Management System (NIIMS). Popularly known as *huduma namba*,[1] the system collates and centralises all identity profiles and identity processes issued and carried out by government agencies. Subsidiary laws under NIIMS mandate issuing a unique personal identifier to each person – citizens, residents and even children. The number – together with biometrics such as fingerprints and iris, earlobe and facial photographs – is required for identification and authentication, prior to accessing government and private services. This could arguably become the most comprehensive surveillance system in Kenya, if the government integrates data sets from government identity systems under *huduma namba* with private data such as mobile phone numbers and social media. It was noted in a judgement following a case contesting *huduma namba* that the government needed to enact an appropriate comprehensive regulatory framework to ensure legal protections (eKLR, 2020b: para. 1047(III)).

1 Swahili for 'service number'.

However, civil society organisations have criticised the Kenyan government for conducting extra-legal surveillance and intercepting communications (Privacy International 2017). They have also raised concern about surveillance of groups such as people with HIV or AIDS, human rights defenders and children (UPR Info 2020; eKLR 2020b: para. 791). In addition, private companies such as mobile network operators have been reluctant to install systems that would give government actors access to subscriber information on their networks. These include the 2012 International Telecommunication Union-supported Network Early Warning System (NEWS), which operators argued would disproportionately affect subscriber privacy, as well as the 2018 Device Management System (DMS), which the communications regulator wanted installed to weed out counterfeit devices. In the case of the DMS, mobile network operator Safaricom was among the parties that went to court to oppose the system, arguing that anti-counterfeiting goals could be achieved using less invasive measures (eKLR 2020a).

This report reviews the legal basis for legitimate surveillance in Kenya and protections provided in law for citizens' right to privacy. It does so by answering a series of 12 questions about surveillance law in Kenya.

1. What reasons does the Kenya government use to justify surveillance?

Motivations for surveillance include prevention of terrorism and serious crimes, national security, anti-corruption, health emergencies and control of hate speech, particularly during election periods. All these are provided for in various laws and practices, which have been developed with local and external influences. For example, following a United Nations (UN) Security Council resolution on suppression of terrorism, Kenya introduced mechanisms for the surveillance of terrorism financing (Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations 2013). Further anti-terrorism-inspired laws were made in December 2014 under the Security Laws Amendment Act. The statute amended several security-related laws to provide for surveillance of persons suspected of serious crimes, as well as terrorism. Finance laws were also amended to strengthen know-your-customer measures, as well as reporting requirements for financial institutions, payment service providers and foreign exchange bureaus.

Under the National Intelligence Service (NIS) Act 2012, protection of national security is among the main reasons for intelligence surveillance. Other rationales for surveillance include prevention of crime and keeping of law and order (National Police Service (NPS) Act 2011, section 51(g)). Anti-corruption and prevention of economic crimes is also cited as a basis for surveillance, although this is not specifically provided for in the anti-corruption law.

Another motivation for surveillance is to protect intellectual property. Private actors such as content owners have attempted to have internet service providers and mobile network operators monitor their networks for content that infringes on their intellectual property rights (Article 19 Eastern Africa 2020). The Communications Authority in 2017 attempted to install a DMS that would connect to mobile network operators' systems to filter out counterfeit devices in the country. The High Court in 2018 declared DMS unconstitutional, but later in 2020 the Court of Appeal allowed the DMS project to recommence and ordered the Communications Authority to subject the proposed DMS guidelines to public participation (eKLR 2020a).

Health surveillance is carried out under the Public Health Act 1986, which was enacted during a time when digital surveillance had not been anticipated. Since the emergence of Covid-19 in Kenya in 2020, the Ministry of Health,

with the aid of the NIS, has been undertaking health surveillance, reportedly through a system that helps with contact tracing (Odhiambo 2020). The Public Health Act does not specifically provide for contact tracing. Initially, the state tracked Covid-19 patients as well as people under quarantine, to ensure that they did not flout movement restriction rules (Olewe 2020). Along the way, a digital tracing app that used geolocation data to track people passing through the country's airports and ports was deployed. Currently, Kenya is collaborating with African health authorities in sharing information about Covid-19 testing and vaccination certification for travellers (Amoth 2021). The Ministry of Health also has a vaccine management system linked to the national identity (ID) card system. This system is among use cases for the national ID, which is increasingly becoming digitalised.

2. Which international conventions protecting privacy has Kenya adopted?

Article 2 of the Constitution of Kenya incorporates international law and obligations as part of domestic law. Kenya has signed the Universal Declaration of Human Rights (UDHR) and ratified the International Covenant on Civil and Political Rights (ICCPR), both of which confer on all citizens the right to privacy and to private correspondence and communication. Regionally, Kenya is also a signatory to the African Charter on Human and Peoples' Rights (ACHPR). Although the ACHPR does not specifically provide for the right to privacy, it provides for dignity of individuals and groups to pursue their development (African Union 1981: articles 5 and 24). Along with other members of the East African Community (EAC), Kenya adopted the EAC Framework for Cyberlaws Phases I and II in 2008 and 2011 respectively (EAC 2008). These frameworks envisage a harmonised cyber environment, with each country expected to adopt laws on data protection as well as cybersecurity.

Kenya has also signed and domesticated UN conventions aimed at addressing terrorism and terrorism financing; and established a financial reporting centre, as well as the Counter Financing of Terrorism Inter-Ministerial Committee under the Prevention of Terrorism Regulations. These regulations create a basis for financial surveillance and reporting.

3. Which domestic laws enable or limit permitted surveillance in Kenya?

Kenya does not have a specific law regulating surveillance, but several laws either prohibit or regulate surveillance. At the highest level, the Constitution protects privacy, including informational privacy. Article 31 frames the right to privacy as including protection from: search and seizure of property; information about family or private affairs being unnecessarily required; and infringement of communications. In addition, article 35 guarantees citizens' right to access to information. This includes information held by the state and others that is necessary for the enjoyment of rights or freedoms.

Both the right to privacy and access to information are among the fundamental rights that can be limited through legislation. Article 24 of the Constitution lists the factors to be taken into account when limiting a right. These include the: nature of the right; purpose of the limitation; nature and extent of the limitation; and a balance between individual enjoyment of rights and the rights and fundamental freedoms of others, whether less restrictive measures to limit the right exist or not. In addition, the Constitution allows for limitation of the right to privacy, among other rights, for members of the Kenya Defence Forces and the NPS (Constitution of Kenya 2010, article 24). For example, police officers' right of access to information is limited, under several justifications, such as protection of classified information, national security, security and integrity of the police service as well as protection of the fundamental rights of others (NPS Act 2011, section 47(2)).

For access to information related to surveillance, the Access to Information Act sets out reasonable grounds under which an access to information request may be denied. These range from national security interests to due process, protection of the privacy of others, protection of commercial interests, including intellectual property, and professional confidentiality (Access to Information Act 2016, section 6). The law further outlines what 'national security' consists of, which includes covert operations, intelligence activities and lawful investigations. However, the law includes a public interest test, where a court may order disclosure of information if the public interest outweighs the harm to protected interests. In addition, requests for information relating to environmental tests override protected interests (Access to Information Act 2016, section 6(4)).

Statutes on surveillance can be broadly classified into laws that prohibit surveillance and those that allow it.

a) Laws prohibiting surveillance

The Kenya Information and Communication Act (KICA) is the primary law on telecommunications and broadcasting. Section 31 penalises unlawful interception of communication by service providers. Section 83 also creates the offence of accessing computer systems for purposes of interception of communication. Consumer protection regulations under KICA also prohibit licensees from monitoring communications.

Unauthorised interception is prohibited under the Computer Misuse and Cybercrimes Act (CMCA) 2018, with stiff penalties of up to 20 million Kenyan shillings (about US$200,000) (section 17). There is also a new crime of interception of mobile money messages in section 31 of the CMCA.

Kenya in 2019 enacted the Data Protection Act, which regulates lawful processing of personal data. The Act generally prohibits processing of personal data without data subjects' consent (section 30).

b) Laws allowing surveillance

The laws allowing surveillance are varied, ranging from communications regulation to anti-money laundering, security and content regulation statutes. More recently, e-government services such as a national system for schoolchildren and a digital ID programme have created databases for easy surveillance.

KICA has provisions for court-mandated search and seizure where a person is suspected to have committed an offence (section 89). Law enforcement officers often rely on this provision to access information from mobile network operators, which are licensed under this Act (Safaricom 2019).

The main law regulating financial surveillance is the Proceeds of Crime and Anti-Money Laundering Act 2009. Financial institutions are required to monitor patterns of cash flowing into financial reporting centres. They must also verify customer identities, keep records of customers, and establish and maintain internal reporting procedures. This has created the basis for electronic surveillance of financial transactions. It has also led to a push for digital ID, which financial institutions can use to validate their customers' ID documents (Breckenridge 2019).

The NIS Act limits the right to privacy by allowing for court-warranted investigations into suspected crimes. Warrants may be issued for monitoring of communications (section 36A). Although the provision does not specify the offences for which surveillance may be undertaken, provisions for court

warrants under the Act are linked to covert intelligence operations. The NIS Act broadly defines offences that may attract covert operations as any 'threats against national security' (section 42). In terms of proportionality, the provision gives broad powers to monitor communication for purposes of preserving national security. Political leaders, as well as Parliament, have severally proposed or directed NIS to carry out intelligence operations on issues such as impropriety in public service, cheap imports in the agricultural sector and public fundraising (Ombati 2020; Otieno and Obala 2020; Ng'ang'a 2021). The provision on covert operations, however, requires a court to issue a warrant before monitoring of communications can begin. A court can only issue an order for surveillance for 180 days, but this can be extended.

Security laws that allow surveillance include the Prevention of Terrorism Act (PTA) 2012, NPS Act, NPS Commission Act, CMCA and Mutual Legal Assistance Act. The PTA permits the investigation and interception of and interference with a person's communications in the course of investigating, detecting or preventing a terrorist act (sections 35, 36 and 36A). Such interception can be carried out by various bodies, with varying levels of adherence to the principle of proportionality. When carried out by the police, there is a pre-authorisation procedure, involving approval by the inspector general of police or director of public prosecutions, as well as a court warrant.

The law also directs the court to analyse the necessity of the application for a warrant, especially since the application for a warrant may be carried out by the police without involving the subject of surveillance. The law also criminalises unauthorised interception by a police officer. However, in a separate provision, the same law authorises interception of communications by national security organs[2] to intercept communications in 'detecting, deterring and disrupting terrorism' (section 36A). This provision does not further delineate how necessity and proportionality are to be achieved, although it empowers the cabinet secretary to make regulations to give effect to the provision.

Under the NPS Act 2011 and NPS Commission Act 2011, the police can collect and provide intelligence on crimes and undertake investigations on serious crimes including cybercrime. The Act further makes provisions for the classification of information (NPS Act 2011, sections 24, 27, 35 and 51).

The CMCA envisages court-warranted interception of 'content data', defined as the substance of a communication, by law enforcement officers in the course of investigating crimes. Under section 53, officers are expected to procure court orders that can also extend to service providers, which

2 Article 239 of the Constitution defines national security organs as the KDF, NIS and NPS.

may be compelled to help with investigations. Section 52 envisages real-time collection of electronic traffic data, where service providers can be compelled to permit law enforcement officers to collect data. Requests for real-time traffic data, as well as content data, can also be made under mutual legal assistance arrangements;[3] these are not locally authorised by courts (sections 63 and 64).

However, the Mutual Legal Assistance Act contains some necessity and proportionality requirements. For interception requests, the Act requires that the requesting state give information on: the criminal conduct under investigation; identification of the subject, with details for the electronic or telecommunication address to be monitored; desired duration of the interception; and the authority requesting the interception. A confirmation of a warrant or lawful interception order from the requesting country is also required. The Act does not provide any other oversight for mutual legal assistance requests; yet once a request is accepted, Kenya may immediately require immediate transmission of interceptions or recording and subsequent transmission of communications to the requesting state (Mutual Legal Assistance Act 2011, section 27).

Content regulation statutes such as the CMCA and the National Cohesion and Integration Act (NCIA) 2008 establish offences that law enforcement bodies use as a basis for surveillance. The CMCA has established offences such as publication of fake news and spreading of false information, while the NCIA prohibits content that may incite ethnic hatred. The NCIA was passed following post-election violence in 2007–08 that led to the deaths of more than 1,200 people and displaced over 500,000. The National Cohesion and Integration Commission (NCIC), which is charged with implementing the NCIA, has invested in surveillance software to monitor election campaign content online (The Nation 2011). During election periods, monitoring of online spaces occurs to identify content that could lead to violence. In 2017, the Communications Authority, in collaboration with the NCIC, issued guidelines on election campaign content disseminated through electronic networks (Communications Authority and NCIC 2017). This was the basis for monitoring SMS text messaging services and social media for what they termed undesirable content. However, there is no specific law mandating digital surveillance for hate speech.

3 Mutual legal assistance is a framework under which a state may request for assistance from another state during criminal investigations. In Kenya, such arrangements are governed under the Mutual Legal Assistance Act 2011, where legal assistance is available to states and international organisations that Kenya has signed agreements with and, in some cases, requesting states, even when there is no prior mutual legal assistance agreement (section 3).

During the Covid-19 pandemic, surveillance has been carried out under the Public Health Act 1986 (section 67). Examples of digital health surveillance include a contact tracing app that integrated public service vehicles (PSV). PSV operators were required to enrol their vehicles on the app using registration numbers and to collect identification card numbers and contact details from every passenger (Oketch 2021; Phillips 2021). The system was later dropped, but other systems (e.g. a testing and vaccine certification system) have been adopted. Civil society organisations have raised concerns over the lack of a legal framework to address the privacy of those whose data is collected, as well as oversight of such surveillance (article 19 2020; Article 19 Eastern Africa, the Kenya ICT Action Network and Pollicy 2021). In the Covid-19 pandemic, people found to be spreading information that was contrary to government reports on both open platforms and private messaging apps were charged with spreading false information under the CMCA (Article 19 2020).

Identity data can also enable government surveillance. The Ministry of Education manages the National Education Management Information System (NEMIS), which records information on all learners in Kenya, including their educational activities. The system issues learners with a unique personal identifier, using their birth certificates and parents' national identity card numbers (Ministry of Education 2017). It is not clear if the system is linked to any other system – for example, *huduma namba* – though law enforcement officers have warned students caught breaking the law that their details will be recorded (Muchunguh 2021).

NEMIS was a precursor of NIIMS, a more comprehensive database that is meant to cover all citizens and residents in Kenya. NIIMS was established in 2019 under the Registration of Persons Act. Subsidiary legislation issued in 2020 makes NIIMS the primary source of identification of all Kenyan citizens/residents in Kenya. This means that through NIIMS, the government can track all the services that a person accesses, from birth to death; for example, mobile phone registration, land registration, health insurance, school enrolment, national examinations and driving records. while the Data Protection Act 2019 prohibits processing of data without the data subject's consent, the Act also lists duties carried out by public bodies as among exceptions to processing without consent. Other exceptions include public interest and exercise of official authority.

4. How does Kenyan surveillance law compare with that in other countries in Africa/US/EU/UK?

The provisions prohibiting surveillance in Kenya – starting from the constitutional provisions on privacy, access to information and limitation of rights – measure up to international standards such as the UDHR, ICCPR and ACHPR. They guarantee protection of fundamental freedoms including the right to privacy. Under article 24 of the 2010 Constitution, laws limiting fundamental rights are required to pass the three-part test of legality, necessity and proportionality. This test, which is elaborated under the Constitution, has been the subject of many lawsuits, with judges testing the laws against considerations such as the nature of the law, whether less repressive means could have been used to achieve the same ends, and whether the law is appropriate for a democratic society.

There is no single law that comprehensively regulates surveillance as is the case in South Africa, the United States (US) and the United Kingdom (UK). However, from the various security legislations – for example, the NIS Act, NPS Act and PTA – a primary reason for surveillance is national security. This is similar to many African countries where intelligence gathering is carried out for protection of national security. Other reasons for surveillance include prevention and investigation of crimes, as well as preventing and countering terrorism.

Without a comprehensive law, surveillance practices go on without a legitimate basis or any oversight. These include mandatory SIM card registration, hate speech monitoring and content regulation in general. This is similar to many other African countries where governments undertake surveillance without specifying a legitimate basis and without oversight (CIPESA 2019: 6).

Similar to the US, where the USA PATRIOT[4] Act was adopted as an anti-terrorism measure, Kenya has enacted the PTA as well as regulations on financial reporting as part of the war on terror. However, as has been argued in cases such as the Coalition for Reform and Democracy (CORD) case, anti-terrorism efforts can easily give rise to mass surveillance as state agencies can use investigation of terrorism to gain access to mobile, internet and financial records (eKLR 2015). The case challenged a raft of amendments to

4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

security laws where the state sought to enhance anti-terrorism investigation by detaining terrorism suspects without charging them, limiting expression and creating a legal basis for covert intelligence operations.

In terms of oversight, Kenyan law has similarities with South African law with regard to seeking administrative and judicial approval of warrants for surveillance. Under the NIS Act, court warrants are required prior to covert operations, similar to the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act *(RICA)* in South Africa. However, the reporting mechanisms differ, in that Kenya has no specific reporting requirements for surveillance activities to parliamentary committees as is the case in South Africa.

5. How does Kenyan surveillance law compare with the UN Draft Legal Instrument?

The UN Draft Legal Instrument on Government-led Surveillance and Privacy recommends that states have a specific statute and oversight on government-led surveillance. The instrument considers surveillance as a limitation to privacy, requiring states to adopt necessity and proportionality in surveillance. Kenya partly aligns with the draft instrument with regard to the intelligence law, but fails in many other respects, including use of digital identity data for surveillance.

Although there is no single statute regulating surveillance, Kenyan laws enacted immediately after the 2010 Constitution – for example, the NIS Act, NPS Act and PTA – acknowledge that surveillance is a limitation to rights such as privacy and access to information. Where a court has authorised surveillance, the laws require an application to the court to list the reasons why law enforcement officers need to infringe on people's privacy.

Use of digital identity data for surveillance has not been well captured in the laws. For example, there are mandatory SIM card registration laws, where the SIM card is linked to the national ID. However, national ID laws do not provide principles or data-sharing codes among civil registries in the country. Civil registries is a term introduced under *huduma namba* regulations. It refers to government agencies that issue identity documents such as birth certificates, passports and education certificates. Since the registries perform duties of a public nature that may be subject to exceptions to the grounds for data processing, it is important that use of their data for surveillance purposes be regulated.

Kenya's surveillance activities often take place under the veil of national security, an area that has traditionally been protected from public scrutiny. The 2010 Constitution defines national security very broadly, encompassing 'internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests' (Constitution of Kenya 2010, article 238(1)). National security is one of the bases for intelligence operations under the NIS Act. National security is also exempted from the Data Protection Act under section 51.

The NIS Act does not provide a specific oversight mechanism for surveillance, but it does provide three mechanisms for oversight of intelligence in general.

The first is a council consisting of three cabinet secretaries, the attorney general, director general of the intelligence service and any other person the president may appoint. The second is parliamentary oversight and the third is a complaints board. The complaints board, which is headed by a person who may serve as a judge, is mandated to receive complaints from any member of the public (NIS Act 2012, pt. VII). The UN Draft Legal Instrument and International Principles on the Application of Human Rights to Communications Surveillance call for an oversight mechanism specific to surveillance that is independent of government and security services; and which has the power to access all surveillance requests and authorisations to verify whether surveillance practice is 'legal, necessary and proportionate' as the Act intended.

While the new laws provide for judicial pre-authorisation, this only occurs in specific cases. The Independent Policing Oversight Authority (IPOA) has a mandate to investigate complaints regarding the police. It is made up of a board of experts from various fields. IPOA annual reports highlight the nature of cases the authority has dealt with since its establishment in 2012. Surveillance is not among the complaints, although complaints such as enforced disappearance can be traced to surveillance (Privacy International 2017). IPOA, along with other human rights institutions, could be strengthened through capacity building on issues of surveillance, to be able to play the role of independent oversight body. Also, laws do not provide for the specifics of surveillance, hence there are no guidelines on any of the surveillance systems in use. There are no recorded human rights impact assessments, even for non-surveillance data such as digital ID.

The right to notification that you have been subject to surveillance – recommended in the UN Draft Legal Instrument and the International Principles on the Application of Human Rights to Communications Surveillance – is not provided for in Kenyan surveillance law. While notification is provided for under data protection laws, surveillance may fall under exceptions to the Act as it is undertaken as a public duty (Data Protection Act 2019, section 51(2)(b)). In addition, the law came into force in 2019 and is in the early stages of implementation. Data subjects have not been provided with mechanisms for asserting their data rights. The right to human assessment in automated decision-making processes is also provided for under the data protection law. However, the public is not aware of decisions which are made by automated means or their right to have such decisions subjected to human assessment. Matters of cross-border data transfer are also provided for under the Data Protection Act.

6. Does legislation provide adequate definitions of key legal terms?

The NIS Act defines national security with reference to the constitutional definition. This definition also applies to all other laws on surveillance. The law specifies privacy rights that are limited and outlines 'purposes for the limitations' in part IV. These include: national security; protection of classified information; discipline and security of intelligence officers; and protection of fundamental freedoms of a person which does not prejudice the rights and freedoms of others (section 32).

Section 48 of the NPS Act provides for limitations of the right to access to information, for similar purposes as described under the NIS Act.

Other key legal terms such as reasonable grounds and legitimate purpose are not defined in law but have been considered by courts. For example, Kenya's experiences with terrorism in the country have created the basis for considering the prevention of terrorism to be a legitimate aim of conducting surveillance. In the wake of terrorist attacks, the 2014 Security Laws Amendment Act was enacted. In a case contesting increased risk to privacy under the NIS Act, the court found anti-terrorism intelligence to be rationally connected to the purpose of 'detection, disruption and prevention of terrorism' (eKLR 2015: para. 308). In this particular case, the High Court found that the provisions for internal pre-authorisation as well as requirements for judicial warrants would provide adequate opportunity for the judicial officer to ensure that there were legitimate aims and reasonable grounds for surveillance.

7. How do legal safeguards, checks and balances, and independent oversight operate in practice?

Existing safeguards such as constitutional and legal provisions have been removed from public scrutiny since there is no mechanism for independent oversight and public reports. This lack of transparency prevents the public from understanding the full extent of surveillance in the country. Reports indicate that Kenya undertakes surveillance, although it is not possible to know the extent to which the law, or international standards such as the UN Draft Legal Instrument, or necessary and proportionate principles are adhered to. Since 2012, the Communications Authority has attempted to install two systems, NEWS and the National Intrusion Detection System (NIDS), on internet service providers' servers. As reported by Privacy International (2017), the surveillance potential of the systems is not proportionate to the stated benefit, which is to monitor cyber threats.

Another example of a system installed without a proper legal framework is the street-level closed-circuit television (CCTV) surveillance system in the capital Nairobi and in Mombasa. The system was installed by mobile network operator Safaricom in collaboration with Chinese telecoms technology manufacturer Huawei. It includes facial recognition technology as well as licence plate readers (Kapiyo and Githaiga 2014; Burt 2018). Despite protests from civil society organisations, there has been no transparency on use of the system and reports indicate that it is running (Mutai 2020). The system was enhanced by integrating all national security communications systems (The Presidency 2020). Regulations on CCTV use were also put out for public consultation but have yet to be gazetted (Ministry of Interior and Coordination of National Government 2019).

Reports on data use for political campaigning during the 2017 elections indicate that political parties obtained data from public and private databases for targeted advertising (Mutung'u 2018). Use of corporate surveillance for political gain undermines democracy, particularly where the incumbent administration also has political control (Nyabola 2020).

National security has often been used as a reason for not openly discussing surveillance practices. For example, in the 2020 statutory annual report on the state of security, the government reported that it had increased surveillance of online spaces to combat threats such as ethnic hatred, student unrest and counterfeit goods. However, further information – such

as on the systems used, action taken against persons of interest, and safeguards – was not provided (Kenyatta 2020: ix, 13, 17).

8. How effective are existing laws and practices in protecting privacy and limiting surveillance?

Although Kenya has constitutional provisions on the right to privacy and access to information, as well as laws on surveillance, these frameworks have not been sufficient to protect the public from unwarranted surveillance. According to a report by Privacy International (2017), law enforcement officers gained access to mobile network operators' data to carry out surveillance on persons of interest. The report tied this surveillance to extrajudicial killings, which led to calls for privacy laws.

However, the Data Protection Act 2019 exempts national security functions from its application. This leaves gaps in areas such as public and private CCTV cameras, which law enforcement agencies can gain access to in the course of their duties, without proper oversight.

The Data Protection Commissioner developed guidelines on data-sharing by private and public entities during the Covid-19 pandemic. However, it is not clear if the guidelines are in operation and there are no records on data-sharing agreements during the pandemic period. This points to the need for the kind of annual public transparency reports recommended by the **International Principles on the Application of Human Rights to Communications Surveillance,** so that citizens and parliamentarians can have confidence that surveillance is being applied in accordance with the law.

9. Are existing surveillance practices in Kenya 'legal, necessary and proportionate'?

The Constitution defines national security as 'the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests' (Constitution of Kenya 2010, article 238). This provision was included during the making of the 2010 Constitution to safeguard against the practice of government overreach affecting human rights on grounds of national security.

Laws made pursuant to national security interests have been the subject of constitutional interpretation, with courts generally supporting national security-related activities unless they violate citizen's rights. For example, following a spate of terrorist attacks in the country from 2013, the government amended several security laws with the aim of specially investigating and prosecuting terrorism cases. In a case instituted by the Coalition for Reform and Democracy (CORD) political party and others, the petitioners argued that the amendments severely affected fundamental rights and freedoms such as privacy, access to information and the right to a fair trial. The court found the sections related to access to justice – such as issues of bail, the right to remain silent and access to evidence to be used against the accused – to be unconstitutional. However, limitations on privacy were found to be justifiable in the fight against terrorism (eKLR 2015).

Lack of transparency or reporting mechanisms make it difficult to analyse how judges have considered surveillance applications from law enforcement. Data from private internet service providers on government requests for access to personal data would also be useful in analysing whether surveillance requests are based on law and whether they are necessary and proportionate.

10. How has surveillance law played out in court in Kenya?

Besides the CORD case, other landmark cases include one challenging the collection of data on HIV-positive people, the petition against the DMS and the *huduma namba* digital identity (NIIMS) case. In the first two instances, the courts ruled in favour of the petitioners, upholding the right to privacy. These two cases were instituted following plans by public agencies to create systems for surveillance. In the third case, which concerned a digital ID system, the court seemed to resign itself to the fact that the country must digitalise. It allowed the system, but ordered that a sufficient and comprehensive framework on issues such as protection of privacy be enacted first.

In 2016, President Uhuru Kenyatta directed national government administrators to collect data on HIV-positive people in their jurisdictions, including children attending school, to streamline the supply of HIV medication. The Kenya Legal & Ethical Issues Network on HIV and AIDS (KELIN), a non-governmental organisation (NGO), challenged the directive on grounds of its proportionality, among other reasons. The organisation argued that collection of biometric data was a violation of privacy that could consequently lead to criminalisation and stigmatisation of already vulnerable people. The court found that, although the government had a legitimate interest, the means of collecting data infringed on people's privacy. Therefore, the directive was declared unconstitutional and the government was ordered to code data that had already been collected (eKLR 2016).

In the DMS cases, mobile network operators and civil society activists protested against the DMS that would have been installed on mobile network operators' systems, to check the authenticity of mobile devices to rid the country of counterfeit devices (Communications Authority 2016). They argued that the system was disproportionate to the mischief the government wanted to cure. The High Court also found that the measures were not necessary because less invasive measures were available that achieved the same ends without violating mobile subscribers' privacy. This decision was, however, subsequently overturned by the Court of Appeal, which ordered the Communications Authority to engage in consultations and also develop guidelines for the project (eKLR 2020a).

Issues of surveillance were part of the CORD case. Petitioners argued that introducing a new provision allowing the NIS to carry out covert operations and interception of communications by national security organs legitimised mass surveillance (eKLR 2015: para. 282). The court, however, took judicial notice of the terrorist attacks that had taken place in the country and found that there was a genuine national security interest – a 'legitimate aim' in the language of the international principles – in monitoring communications to prevent further attacks. With regard to intelligence, it found that the pre-authorisation by a judge, time-limited warrants and criminalisation of unlawful surveillance were sufficient safeguards to privacy. The court emphasised that, given the nature of terrorism, it was justifiable for the government to carry out surveillance, after obtaining court orders. In addition, the court found that the parties had not demonstrated less restrictive ways of achieving the national security purposes of the surveillance law (*ibid.*: para. 308). Notably, petitioners in the CORD case did not canvass issues of oversight and accountability of surveillance. As was the case in the South African case *AmaBhungane Centre for Investigative Journalism v. Minister of Justice and Minister of Police,* the court decried the opaque nature of surveillance orders (Constitutional Court of South Africa 2021).

11. What is working? What gaps are there in existing policy, practice, knowledge and capacity?

The right to privacy under Kenya's Constitution is well provided for. It includes privacy of information as well as communications. Further, the Constitution has domesticated the legitimacy, necessity and proportionality principles under international law by providing guidelines on how rights such as privacy may be limited. However, the laws under which surveillance is undertaken do not always provide a legitimate basis for surveillance.

Issues of surveillance have been the subject of litigation and courts have upheld the right to privacy in some cases. However, litigation cannot be a sustainable means of protecting the rights of people, with increasing government-led surveillance. A comprehensive law is therefore needed to narrowly define legitimate grounds for surveillance.

Where the private sector is involved, transparency reports by technology companies such as Google are important in bringing to the fore issues of surveillance. People would otherwise not be aware that law enforcement officers surveil their private communications or have any means of appeal or redress. However, not all companies provide reports and, even in the case of Google, not all requests for information are published (Google 2021).

National human rights institutions such as the Kenya National Commission on Human Rights (KNCHR) have not been pursuing digital rights. For example, annual and general reports of such institutions in the past few years have not highlighted the impact of electronic surveillance on fundamental rights. While a 2021 submission to the UN Human Rights Committee raised concerns about the implementation of the PTA being used to shrink civic space, it does not sufficiently link this to digital surveillance. Linkage of surveillance to fundamental rights would be a positive step in making surveillance actors more accountable, since the KNCHR has a general oversight mandate for all state organs.

Issues of surveillance should receive more attention in Parliament. Parliamentary committees on security should provide reports on emerging issues including procurement of surveillance systems. For such oversight to be meaningful, parliamentarians' capacity on issues of surveillance should be built. Researchers and civil society organisations working on surveillance and human rights should therefore disseminate their research findings to parliamentarians, who could serve as a useful mechanism for seeking

information on surveillance programmes. Parliament could also contribute to transparency, and provide oversight and accountability.

Lack of transparency is a problem. Mandatory SIM card registration, for example, has been faulted by several civil society organisations. During Kenya's 2019 universal periodic review by UN mechanisms, mandatory SIM registrations were linked with surveillance of human rights defenders (UPR Info 2020). Whereas national security is used as a reason for requiring registration of the SIM cards, registration has been cited as providing law enforcement officers direct access to telecommunications networks. Networks do not publish information on government requests for such access (*ibid.*).

12. What recommendations arise for future legislation, practice, or further research?

- Surveillance systems such as hate speech monitoring and anti-corruption are implemented in a legal vacuum, contrary to the guidance of the UN Draft Legal Instrument. Kenya should enact a specific surveillance law prior to purchasing or developing surveillance systems. The law should cover both surveillance systems and use of non-surveillance systems such as digital ID for surveillance purposes. As surveillance is a limitation on human rights, the surveillance law should adhere to the constitutional requirement for legality, necessity and proportionality.
- While Kenya currently has a system for judicial authorisation for some types of surveillance, the system is still lacking in that there is no independent oversight body to supervise surveillance practice. Mechanisms for public accountability, such as transparency reports, are also lacking.
- Existing – and future – surveillance systems should undergo human rights impact analysis. All surveillance actors should develop mitigation measures for the people whose rights surveillance systems affect. Measures could include notification of surveillance subjects, removal from surveillance and independent review of surveillance activities.
- The law should adopt surveillance principles in the UN Draft Legal Instrument, especially on transparency of surveillance and accountability of surveillance actors. Issues requiring transparency include notification of surveillance subjects as well as publication of surveillance reports. Issues of accountability include retirement of surveillance data, so that surveillance subjects are not perpetually in government files. Similarly, health surveillance data collected during the Covid-19 pandemic should be retired once the pandemic is over.
- There should be greater protection of special interest groups such as children and people with HIV or AIDS. Mass surveillance of such groups should be specifically outlawed; and where surveillance is applied for, the requesting authority should be required to indicate to the judge whether the subject is from a protected category.
- The National Security Council should provide information on the nature of surveillance in Kenya, actors, statistics on surveillance activities and their value. In tandem, private companies involved in

surveillance such as telecommunications network operators should publish periodic reports on government surveillance requests.

- Information on health surveillance during the Covid-19 pandemic should be published. People who accessed the information as part of the pandemic response – for example, app developers – should also be required to retire that data or at least de-identify it to protect the privacy of the public.
- The NPS Act should have narrower provisions on surveillance to meet the legitimate aims and reasonable grounds recommended by international law. These should include the basis for surveillance, types of crimes that attract surveillance as well as internal and independent external oversight on surveillance activities.
- Surveillance carried out under other laws such as the Anti-Corruption and Economic Crimes Act, Kenya Revenue Authority Act, and National Cohesion and Integration Act should be contested for their lack of legitimate aims and accountability.
- All surveillance laws should have a reporting mechanism whereby Parliament and the public are made aware of the statistics, nature and value of surveillance in a given period. Subjects of surveillance should also be notified of surveillance even if this is after the fact.

Who needs more capacity to do what? Journalists, academics, researchers

- The KNCHR should extend its monitoring to surveillance activities of the various government and private bodies.
- Security researchers should be sensitised on human rights aspects of surveillance for groups such as children and people with HIV or AIDS.
- More awareness should be created about the impact of digital surveillance among the public, in general, and groups such as human rights defenders and journalists, in particular.

What additional research is needed into which areas?

- More research is needed on the impact of surveillance on groups. How can group rights impact assessments be done? How can mechanisms such as the UN Draft Legal Instrument incorporate group rights and, where groups' rights are affected, impose higher sanctions?

References

African Union (1981) ***African Charter on Human and Peoples' Rights*** (accessed 4 August 2021)

amaBhungane Centre for Investigative Journalism and Stephen Patrick Sole v. Minister of Justice and Correctional Services and Nine Others (2021) ***Constitutional Court of South Africa. Case CCT 278/19*** (accessed 10 August 2021)

Amoth, P. (2021) ***Guide on the Digital Verification of COVID-19 Certificates,*** Pretoria: Ministry of Health (accessed 4 August 2021)

Article 19 Eastern Africa (2020) ***'Kenya: Intellectual Property Bill Must Not Water Down Freedom of Expression Protections'***, Article 19, 5 June (accessed 10 August 2021)

Article 19 Eastern Africa; the Kenya ICT Action Network and Pollicy (2021) ***Unseen Eyes, Unheard Stories: Surveillance, Data Protection, and Freedom of Expression in Kenya and Uganda During COVID-19***, Article 19 (accessed 4 August 2021)

Boinett, B.W. (2009) **'The Origins of the Intelligence System of Kenya'**, in S. Africa and J. Kwadjo (eds), *Changing Intelligence Dynamics in Africa,* Birmingham: Global Facilitation Network for Security Sector Reform (accessed 18 September 2021)

Breckenridge, K. (2019) **'The Failure of the "Single Source of Truth About Kenyans": The NDRS, Collateral Mysteries and the Safaricom Monopoly'**, *African Studies* 78.1: 91–111 (accessed 18 September 2021)

Burt, C. (2018) ***'Kenyan Police Launch Facial Recognition on Urban CCTV Network'***, BiometricUpdate.com, 24 September (accessed 21 June 2021)

CIPESA (2019) ***Digital Rights in Africa: Challenges and Policy Options***, Kampala: Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (accessed 30 June 2021)

Communications Authority (2018) **Press Statement by Mr Francis W Wangusi, Director General, Communications Authority of Kenya (CA), on Misleading Media Reports Regarding the Regulatory Tool for Curbing Counterfeit Devices on Mobile Networks** (accessed 29 July 2021)

Communications Authority (2016) ***Tender Advert for Design, Supply, Delivery, Installation, Testing, Commissioning and Maintenance of a Device Management System (DMS)***, Nairobi: Communications Authority of Kenya (accessed 31 July 2021)

Communications Authority and National Cohesion and Integration Commission (NCIC) (2017) ***Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content Via Electronic Networks*** (accessed 30 June 2021)

eKLR (2020a) ***Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others*** (accessed 21 June 2021)

eKLR (2020b) ***Nubian Rights Forum and 2 others v Attorney-General and 6 others; Child Welfare Society and 8 others (Interested Parties)*** (accessed 13 August 2021)

eKLR (2016) ***Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others*** (accessed 13 August 2021)

East African Community (EAC) (2008) ***Draft EAC Legal Framework for Cyberlaws***, UNCTAD and EAC (accessed 10 August 2021)

eKLR (2015) ***Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya &10 others*** (accessed 13 August 2021)

Google (2021) **Government Requests to Remove Content – Kenya** (accessed 13 August 2021)

Kapiyo, V. and Githaiga, G. (2014) **'Is Surveillance a Panacea to Kenya's Security Threats?'**, in *Communications Surveillance in the Digital Age,* Global Information Society Watch (accessed 21 June 2021)

Kenyatta, U. (2020) ***Annual Report to Parliament on the State of National Security. Statutory report. Parliament of Kenya***, Nairobi: Republic of Kenya, Executive Office of the President (accessed 21 June 2021)

Lind, J.; Mutahi, P. and Oosterom, M. (2015) ***Addressing and Mitigating Violence. Tangled Ties: Al-Shabaab and Political Volatility in Kenya***, IDS Evidence Report 130, Brighton: Institute of Development Studies (accessed 10 August 2021)

Ministry of Education (2017) ***NEMIS User Guide***, Nairobi: Ministry of Education (accessed 10 August 2021)

Ministry of Interior and Coordination of National Government (2019) ***Public Participation on National CCTV Policy*** Nairobi: Ministry of Interior and Coordination of National Government (accessed 21 June 2021)

Muchunguh, D. (2021) **'DCI to Keep Records of Students Involved in Crime'**, *Daily Nation,* 26 January (accessed 26 January 2021)

Mutai, E. (2020) **'State Releases Sh1.5bn for Safaricom's Police Cameras Deal'**, *Business Daily,* 29 June (accessed 21 June 2021)

Mutung'u, G. (2018) ***The Influence Industry. Data and Digital Election Campaigning in Kenya***, Policy Paper, Tactical Technology Collective (accessed 4 August 2021)

Ng'ang'a, G. (2020) **'Security Organs Could Have Say on Harambees'**, *The Standard,* 19 October (accessed 4 August 2021)

Nyabola, N. (2020) **'Cambridge Analytica and the End of Elections'**, *Al Jazeera*, 18 January (accessed 30 June 2021)

Odhiambo, M. (2020) **'Sh40bn Allocated to Corona Response – Treasury CS Yatani'**, *The Star,* 22 April (accessed 30 June 2021)

Oketch, A. (2021) **'Kenya: Covid-19 Contact Tracing Made Easy By Tech'**, *Daily Nation*, 17 January (accessed 30 June 2021)

Olewe, D. (2020) **'Coronavirus in Africa: Whipping, Shooting and Snooping'**, BBC News, 9 April (accessed 4 August 2021)

Ombati, C. (2020) **'NIS to Lead in War Against Cartel Capture in Public Service – BBI'**, *The Standard,* 26 October (accessed 4 August 2021)

Otieno, R. and Obala, R. (2020) **'"I'll Make No Pact With Evildoers Nor Show Mercy to the Corrupt"'**, *The Standard*, 15 January (accessed 4 August 2021)

Phillips, T. (2021) **'Kenya to Combine Cashless Payments With Covid Contact Tracing on Matatu Minibuses'**, NFCW, 11 January (accessed 30 June 2021)

Privacy International (2017) ***Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya***, London: Privacy International (accessed 21 June 2021)

Republic of Kenya (2015) ***Kenya Information and Communications (Registration of SIM-Cards) Regulations, Legal Notice No 163 of 2015***, Nairobi: Communications Authority of Kenya (accessed 10 August 2021)

Safaricom (2019) **Safaricom Data Privacy Statement** (accessed 4 August 2021)

The Nation (2011) **'NCIC Monitoring SMS, Web Chatter for Hate Speech'**, *Daily Nation*, 5 May (accessed 30 June 2021)

The Presidency (2020) **'President Kenyatta Inaugurates the National Security Telecommunications Service'** (accessed 21 June 2021)

UPR Info (2020) **'Review on 23 January 2020 – Civil Society and Other Submissions'** (accessed 21 June 2021)