Digital Surveillance and Privacy Concerns in the Counter Terrorism Discourse in Kenya: Policy Implications

Fathima Azmiya Badurdeen
Technical University of Mombasa, Kenya

Abstract

Revelations by National Security Agency whistleblower Edward Snowden demonstrated the extent of digital surveillance carried out by different security and intelligence agencies globally. Similarly, in the Kenyan context, human rights organizations revealed concerns on the legality of digital surveillance, the extent of state interference in public life, and the protection of civil rights in the context of national security. The article answers the research question, 'how can digital surveillance as a counter terrorism strategy be balanced with the rights to privacy in Kenya?' This involves a discussion on the state's justification on the use of digital surveillance and its impact on the right to privacy of citizens. To address the main research question the article traced the forces and dynamics which shapes digital surveillance as a counter terrorism strategy in Kenya. The article emphasizes the need for advocating privacy rights, and a fundamental review of digital surveillance practices in Kenya. In an attempt to minimize the impact of digital surveillance on the right to privacy in Kenya, the article recommends for an adoption of policy relevant best practices which balances the two rights: the right to privacy and the right to security. The successful implementation of digital surveillance should be empirically driven with effective public participation in surveillance policy making.

Keywords: Digital surveillance, privacy rights, policy, counter terrorism, legislation

Introduction

On 27 March 2015, Ms. Khadija Abubakar Abdulkadir, Ms. Maryam Said Aboud and Ms, Ummulkhayr Sadri Abdulla were arrested by the Kenya Defence Forces (KDF) at El Wak, a Kenyan town less than 10km from the Somali border (Juma, 2015). They were allerged on terrorism charges for conspiracy with foreigners to carry out a terrorist act in Kenya (Mkongo, 2015). This case of the three ladies were further strengthened with new cyber intelligence reports which revealed that they had contacts in Canada, Qatar, Sri Lanka, Rwanda, Tanzania, Sudan, UAE, Turkey, UK and the US. Accordingly, the recovered information from their laptops, pointed to the fact that the contacts were used to recruit members for al-Shabaab abroad. Evidence recovered from their laptops revealed that the accused had contacts with al-Shabaab linked Mr. Shwaid Mubarak. Pictures retrieved from their laptops contained materials promoting Jihadism and the killing of non-believers, which were alleged to be used for recruitment purposes (Rachel, 2015). Reportedly, the accused ladies were in contact for months with an alleged al-Shabaab member through social media who had arranged their travel (Juma, 2015). This case was one among the many cases which revealed recruitment aided through online means showing the increased trend of transnational terrorism in Kenya with the tendency to exploit cyber space for terrorist purposes. During the trial, the defence challenged several aspects of the prosecution, which included arguments related to constitutional rights based on pretrial detentions to avail time to gather evidence. Further discussions centered on the unclear nature of data been gathered for the trial which included access into personal laptops and mobile phones. Amidst the invoked arguments, the three ladies with another, Halima Adan Ali were convicted on terrorism related charges of being members of a terrorist group, aiding activities related to terrorism (Agnon, 2016). The case brought forth arguments on the perspective of upholding privacy rights amidst a known context for national security if the accused were planning or was intending to join the terrorist group which directly threatened Kenya. The revelations from this case exposed the sheer capacity of the state to collect personal data considered vital to the investigations (Rachel, 2015) while questioning the context of rights involved in the investigation process.

Terrorist use of the online technology for terrorist activities of propaganda, recruitment and attack planning is well emphasized. The United Nations Office on Drugs and Crime Report on 'The Use of the Internet for Terrorist Purposes' (2012) and the RAND report on Radicalization in the digital era (Von Behr, Reding, Edwards, & Gribbon, 2013) had provided a number of cases on how defendants used the internet and related online technologies for terrorist activities. These new trends in terrorist activities and online technologies in terrorism related cases opens up an array of discussions on understanding trends of online usage in terrorist activities and the need for specific skills and techniques in finding terrorism-related content on the internet, and the need for new investigating and prosecuting techniques along with the rights the accused may have during the investigation and prosecution process. Within this context, the protection of privacy rights and other correlated rights had been emphasized (Kuner, 2013).

Using Kenya as a case study, this article explores the power of the state to carry out digital surveillance programmes to counter terrorism without infringing the right to privacy. In an attempt to address this research objective, the article is divided into four sections. Following the introduction, the first section outlines the definitions and the theorizing of the two main concepts: digital surveillance and privacy in the wake of countering terrorism. The second

section develops an analysis of the nature of digital surveillance in the milieu of terrorist usage of the internet and related technology in Kenya. The third section outlines the challenges raised by the spread of digital surveillance in the realms of privacy concerns in the fight against the Kenyan war on terror. The final section synthesizes the analysis to comprehend the clash between the digital surveillance milieu in counter terrorism and the infringement on privacy rights and its implications. Appropriate recommendations were derived from the analysis of the study. The scope of the discussion is limited to the Kenyan context, however could be related to most African countries grappling with countering terrorism online. The methodology for this article comprised of primary research data drawn from the authors PhD study as well as authors involvement in counter terrorism work in Kenya. This included in-depth interviews from stakeholders such as youth, law enforcement officials and other key stakeholders, observations on trials of cases of terror suspects (mainly suspects involved in cyber terrorism propaganda), proceedings and supplementary secondary data from analysis of online terror propaganda materials and sites.

Digital surveillance and Privacy in the counter terrorism discourse

Digital surveillance encompasses a broad range of activities conducted with the intent of gathering intelligence including audiovisual observations to the interception of electronic communications, the collection, processing, storage or transfer of data to third parties (Milanovic, 2015). The Electronic Frontier Foundation (2014) defined digital communications surveillance as broad range of activities that implicates the privacy and expressive value inherent in communications networks. Based on this purview, digital surveillance is viewed with regard to countering terrorism through the gathering of information on individuals (suspected individuals or at risk). Surveillance ranges from human and technologically gazing, where officials watch physical movements and activities of persons; observations used for identification or may act to advance an investigation as a component of a larger body of evidence (CCTV data); or the acquisition of personal data (biometrics, biographical, personal communications and, electronic transactions. This voice or documentary information is then used in criminal investigation or prosecutions. Hence the meaning given to digital surveillance in this article is the digital communications surveyed by the law enforcement (police) on official gathering of information on persons for the purposes of preventing, countering and combating terrorism or prosecuting terror offenders. As digital communications is inspected by the police, the ability to gather more personal information through surveillance searches, and seizure is evident where a great number of persons come within their official scrutiny through suspicion profiles, threat assessments or specific investigations.

The studies on surveillance had been evolving to accommodate the pace of the technological changes. Further, online recruitment and radicalization for terrorism entail the need for surveillance among strategies of countering terrorism, which involves digital surveillance in this digital era. Surveillance can be defined as ‘any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered (Lyon 2001: 2). Historically surveillance functioned as a necessary aspect of maintaining the society. As propounded by Lyon (2007: 14) surveillance was the ‘focused, systematic, and routine attention to personal details for purposes of influence, management, protection or direction. Hence surveillance has constituted to be the core security strategy of many nation states (Sparrow, 2014).

Technological advancement of sensing and recording has resulted in monitoring of individuals and groups without the need for constant direct observations (Gandy, 1993; Lyon, 1994; Lionos, 2003). This new surveillance is characterized by the use of 'technical means to extract or create personal data' (Marx, 2002). Today the 'digital' within the 'new surveillance' have to an extent replaced the bureaucratic and electromechanical surveillance systems. Jones (2001) highlights this digital context as 'digital rule' in surveillance. The digitization of surveillance has two significant reasons: first, is the compression of the time factor that is facilitating monitoring of individuals and contexts across widening geographical distances with little time delays (Lyon, 1994). Second, the aspect of automation (Lianos & Douglas, 2000) where the sorting, identification, prioritization and tracking of bodies, behaviours and characteristics of population under concern is continuous and in real time basis. The automation process due to digitization has replaced the role of human operators to operators who merely program, supervise and maintain systems. This provides immense potential for pervasive surveillance due to digitization that facilitates a change in power, intensity and scope of surveillance (Graham & Wood, 2003). The digitization of surveillance technologies are both quantitative (in terms of size, speed, intensity, coverage) and also qualitative (storage, transmission and computation) (Introna & Wood, 2004). The increase in modern transnational crimes and terrorism within a global technologically fluid environment obligate the law enforcement officials to ensure greater public safety under increasingly unpredictable circumstances (Bloss, 2007). Hence justifying preventive law enforcement in response to the greater use of surveillance to counter and combat transnational threats and the prosecution of transnational offenders.

Therefore, in order to deter terrorist acts states need to gather or supervise different types of personnel electronic information or communication for national security purposes (Weimann, 2006). Digital surveillance is targeted to obtain information in the form of the content of communication, or supervise internet traffic to understand the knowledge of how the terrorist organization functions or behaves, which may include the communication origin, duration, type, time, size, route. Finally, the subscriber data, which includes the personal data of the individual (Oriji, 2014). Further, knowledge of the terrorist organization is gathered from different websites, chat rooms and other internet communications. This includes passive monitoring of websites for intelligence purposes, engaging with individual users in different chat rooms to gather information, shutting down websites or even individual Facebook pages. With advance in technology, new sophisticated tools have been developed to detect, prevent and deter terrorist activities online (RAND, 2013). Dataveillance which is the monitoring of data traits when performing transactions, computer facial photographs, DNA and fingerprints are some other developments in this field of digital surveillance (Palmer, Warren & Miller, 2014).

The right to privacy in the counter terrorism discourse

Inherent to the discussion on digital surveillance is the question of the right for privacy. In 2013, Edward Snowden's revelations on United States and United Kingdom intelligence agencies on conducting indiscriminate and clandestine mass surveillance sparked a global outrage over the violations of privacy rights raising several legal and policy questions regarding the protection of rights to privacy (Mahmoud & Zeki, 2016; Simcox, 2015). The right to privacy is a fundamental human right that protects the privacy of individuals from unwanted intrusions by the State or any other private actor (Kuner, 2013).

The right to privacy faces varied challenges in the context of countering terrorism. The Report of the Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, focused on the right to privacy as a human right in the counter terrorism context. The report defined privacy as a fundamental human right where individuals are provided with an 'area of autonomous development, integration and liberty' (Human Rights Council, 2009). The origins of privacy as a distinct legal concept can be traced to the article, 'The Right to Privacy' by Samuel Warren and Louis Brandeis in 1980. The article was based on a court case in which photography was used to collect information on an individual without consent. The basic concept of the right remains valid amidst the changing dynamics of technology. The legal basis for the right to privacy is found in the 1948 Universal Declaration of Human Rights (Article 21), International Covenant on Civil and Political Rights in 1966 (Article 17), 1950 European Convention on Human Rights (Article 11) and the 1990 Cairo Declaration on Human Rights in Islam (Article 18). All these conventions recognize privacy as an integral part in private life.

However, in the African context, the African Charter on Human and People's Rights do not recognize the right to privacy explicitly (Oriji, 2016), but Article 10 of the African Charter on the Rights and Welfare of the Child provides for the right to privacy. Further, the legal basis for protecting the right to privacy exists under the national constitution of African states such as the section 37 of the Nigerian Constitution. Here, the right to privacy provides the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. In Kenya, Article 31 of the Constitution establishes the right to privacy which provides that "every person has the right to privacy, which includes the right not to have (a) their person, home or property searched; (b) their possessions seized (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed." The right to privacy is further highlighted under Article 2 of the Kenyan constitution that states Kenya's international obligations such as the commitment to the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights which include privacy rights are as part of Kenyan domestic law (Global Privacy Network, 2016). In spite of this stated right for privacy, the expansion of surveillance technologies, the technical capability of the government to intrude into personal lives had 'sought to maintain a principled balance between the needs of law enforcement and democratic freedoms' (National Research Council, 2008).

However, privacy rights are rarely absolute. As expressed under the International law, the Universal Declaration of Human Rights also limits the right to privacy in Article 29(2), in exercising fundamental rights and freedom: 'everyone shall be subjected only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society'. Limitations to privacy exist in African constitutions as well. Under section 45(1) of the Nigerian Constitution, the right to privacy can be restricted in the 'interest of defense, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedom of other persons'. In the Ghanian context, the constitution limits on privacy rights focuses on public safety, the economic well-being of the country, the protection of health or morals, the prevention of disorder or crime or for the protection of the rights or freedoms of others. In Kenya, Article 24 of the Constitution limits this right: A right or fundamental freedom in the Bill of Rights, 'shall not be limited except by law,

and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including: the nature of the right or fundamental freedom; the importance of the purpose of the limitation; the nature and extent of the limitation; the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose' (The Constitution of Kenya, 2010).

Hence, these legal limitations on privacy rights are considered in the best interest on the need to protect the public interest with regard to public security. Public security involves the assisting of law enforcement officials in countering crime, and in this case, countering terrorism. In this regard, gathering intelligence for the purpose of national security is subject to legal limitations allowing states to conduct digital surveillance activities such as intercepting, monitoring and recording private communications. The context of national security provides a legal basis for states to establish laws which enables law enforcement officials to engage in the surveillance of private digital communications.

Digital Surveillance and Counter terrorism in Kenya

Kenya, provides an ideal case study for digital surveillance with the visibility of an increase in digital surveillance technologies and processes in response to countering terrorism and other related cyber crimes. Kenya, with a relatively developed economy, an interactive hub for the east and west in the East African region and with borders to unstable neighbours is grappling with various forms of terrorism. Among such transnational terrorist networks is the Somali affiliated Jihadi transnational terrorist network al-Shabaab. Al-Shabaab has been instrumental in many attacks in Kenya and the rest of the world, mainly in the East African region. Since the KDF (Kenya Defense Forces) intervention into Somalia there have been sporadic attacks by the al-Shabaab in the Kenyan soil. These include the Westgate attack in 2013 (Miller 2013), Mpeketoni attacks in 2014 (Anderson 2014) and terror attacks in Mandera (Al Jazeera 2014) among many other attacks. Further, youth radicalization and recruitment from Kenya are serious concerns associated to this transnational terrorist network (Badurdeen 2012). Contemporarily, the ISIS threat in terms of radicalization and recruitment of youth is eminent in Kenya. For example, among the recent cases being of Mr. Mohamed Abdi Ali, a medical doctor in Wote, Makueni county was allerged on planning to carry out a biological attack in Kenya with his wife, Nuseiba Mohamed Haji Osman who was also a medic. They were also involved in youth recruitment for the ISIS (The Star, 2016).

Apart from the terrorism threat, technological advancement has brought in changes in surveillance practices thereby contributing to the ability of the state to engage in electronic surveillance of citizens. Electronic communications through platforms such as the internet, cellular telephones, and wireless transmissions are intercepted with ease and less physical intrusion (Hier 2003). In Kenya, keeping pace with technology becomes of paramount importance as transnational terrorists rely heavily on technological advancement (Badurdeen 2016). Platforms such as Facebook, Twitter and Youtube have been used by transnational terrorist networks in the dissemination of propaganda materials, the recruitment of new personnel, the dissemination of terror tactics and the planning of attacks (Khader 2016).

Badurdeen (2016) highlighted that in Kenya, the dynamics of physical recruitment of direct one to one in public and private spaces has changed due to the of surveillance of public spaces and improvements in the community policing aspects. Nevertheless, research has revealed that the high use of social networking sites among youth had facilitated a change in the recruitment strategy compared to the past one-to-one physical recruitment. As highlighted by a youth participant,

> *the use of phones has complicated how many young people think and do things. Everything is one click away. Just like how they use the phone on a daily basis, radical messages are also promoted with ease. It's not easy to monitor them. Access to phone and internet makes the entire process complicated. It also changes the dynamics of the poor youth being recruited than the rich youth. Now, both the rich and poor youth are vulnerable. Many can afford these technologies with ease' (Interviewee, 17 January 2016, Mombasa).*

Few things can be highlighted from the above statement. Firstly, the use of phones and internet are wide spreading due to its affordability. Second, internet technologies are also becoming affordable for many youths. Together, the phone and the internet becomes a tool that can be used with ease. The importance of social network sites among youth becomes a tool exploited by terrorist recruiters where messages are posted online. Third, phones and internet penetration have changed the notion that only low income youth are vulnerable for recruitment into terrorist organizations. High income youth categories are equally vulnerable, bringing an equal risk for youths from all income backgrounds.

Within this expansion of digital space and online terrorism recruitment, the Kenyan police are legally authorized to conduct digital surveillance where increasing surveillance are linked to preventing purposes of gathering information on person perceived to be terrorist threats (Mohochi 2011; Mwazighe 2012). The Kenyan laws have given more power to conduct surveillance activities involving criminal and countering terrorism measures (The Security Laws Amendments Act 2014; Rispoli 2015). In Kenya, socio-political and legal changes in a security backdrop have paved a way for an escalation of surveillance by security agencies. Impetus to such high surveillance is the culmination of factors such as transnational terrorism and crime threats and electronic technology in terms of public safety, crime control and public threat assessment (Chumba et al. 2016; Ramah 2014). Richardson (2016) have hailed better legislations and information gathering by the security forces as contributing factors for the decline in terror attacks. Hence, such spread of technologies have necessitated the Kenyan police to ask for greater surveillance and search powers in an order to keep pace with the technology use of terror networks. This was ascertained by the following interviewee, 'wire tapings, online surveillance through face books and twitter accounts become a necessity in countering terrorism. During the past few months alone, these methods of information gathering have helped us foil terror attacks by being proactive' (Interviewee, Mombasa, 2 April 2016). Another participant stated that it gives an idea of their strategy: *'sometimes it gives particular hints of their next step…sometimes it can be a warning, or sometimes it can be knowledge of a particular strategy they intend to adopt…'* (Interviewee, Mombasa, 6 May 2016).

The reasons explained by law enforcement officials included predicting behaviours of radicals and learning the radicalization process as expressed as follows: *'…it allows us to learn their*

close friends, their behaviours, their way of life…it facilitates understanding the radicalized youth or youth in the process of being radicalized…' (Interviewee, Mombasa, 16 February 2016). This was further reiterated by the following interviewee:

> *There are times when we find online evidence of particular face book or Twitter accounts that are used for dissemination of propaganda purposes or to recruit young people. In some cases we just block the site. Our intention is to follow the members or sometimes simply to confuse the network, so that it may take some time for them to build up a support or sympathizer base again. It's a form of prevention… (Interviewee, Mombasa, 9 April 2016).*

Increasingly, the adoption of electronic surveillance is to keep pace with technology and pursue crimes on a global scale across transnational linkages. The Government of Kenya employed different types of digital surveillance. In April 2014, under the Umoja Kenya Initiative, the biometric registration process did collect all data pertaining to an individual including name, age, and identities of relatives, property owned and residence. In May 2014, the government announced that the partially state-owned Kenyan communications provider Safaricom had been awarded a government tender to set up a new surveillance system on CCTV for the Kenyan Police, known as the Integrated Public Safety Communication and Surveillance System. In March 2012, the telecommunications industry regulator, the Communications Commission of Kenya (CCK), announced that it was setting up a system to allow the authorities to monitor incoming and outgoing digital communications. CCK requested that all telecommunication service providers cooperate in the installation of internet traffic monitoring equipment known as the Network Early Warning System (NEWS). The CCK cited a rise in cyber security threats as a justification for this move. In May 2014, the Intercept reported that a programme of the US National Security Agency (NSA) called MYSTIC secretly monitored the telecommunications systems of several countries including Kenya, where the system was known as DUSKPALLET. The programme was described in internal documents as a "program for embedded collection systems overtly installed on target networks, predominantly for the collection and processing of wireless/mobile communications networks." Evidence provided to The Intercept shows that the programme dates back to 2013, and that data gathered through it has been used to generate intelligence reports (Global Privacy Network 2016). Within these surveillance mechanisms, transformations in surveillance practices, privacy laws and public privacy expectations have been of great concern (Human Rights Watch 2014). As highlighted by the Global Privacy Network (2016):

> *…it is difficult to work on privacy and surveillance in the country as the issue is not widely deemed important by society in general. This is in part because of the increased number of security threats, which have enabled a strong national security discourse to overshadow concerns about privacy. Privacy is often considered subsumed to other human rights issues.*

Various safeguards on Surveillance are in operation such as Article 31 of the Kenya Information and Communications Act (2009) which prohibits the unlawful interception of communications by service providers. Further, section 15(1) of the Act states that:

> *Subject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any*

subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data.

Nevertheless, some legal provisions have been made to enhance the powers of law enforcement officials to engage in digital surveillance:
1. Section 45 of the National Intelligence Service (NIS) Act (Act No. 28 of 2012) states that a warrant issued under the Act may authorize any member of the NIS to obtain any information, material, record, document or thing and for that purpose: to enter any place, or obtain access to anything; to search for or remove or return, examine, take extracts form, make copies of or record in any other manner the information, material, record, document or things; to monitor communication; or to install, maintain or remove anything.
2. Section 36 (1), (2) and (3) of the Prevention of Terrorism Act (Act No. 30 of 2012) provides for the interception of communication order, where communication service providers are required to intercept and retain specified communication received or transmitted or about to be received or transmitted by the communication service provider. It also provides fr authorizing a police officer to enter premises and to install any devices for the interception and retention of a specified communication and to remove and retain such device.
3. The Mutual Legal Assistance(MLA) Act (CAP. 75A Laws of Kenya) establishes provisions for a requesting State to make request to Kenya for the interception and immediate transmission of telecommunications or the interception, recording and subsequent transmission of telecommunications. Under section 27 of the MLA Act, it is provided that for the purpose of criminal investigation, Kenya may in accordance with the provisions of the Act and any other relevant law, execute a request from a requesting State for the interception and immediate transmission of telecommunications or the interception, recording and subsequent transmission of telecommunications. Section 32(1) of the MLA Act also provides that a request may be made to Kenya from a requesting State for the deployment of covert electronic surveillance.

Are we Compromising Privacy within the Digital Surveillance Discourse?
One of the most identifiable consequences of increased digital surveillance has been the creation of new privacy boundaries. As highlighted by Bloss (1996 as cited in Bloss 2007) there is an inverse relationship between surveillance and individual privacy. As surveillance increases, individual privacy declines. Increased counter terrorism measures have facilitated widened surveillance and search powers with sophisticated electronic technologies for collecting data on physical and electronic selves (i.e. biometric and virtual identity, expressions and personal data (O'Harrow, 2005). The identities of individuals are becoming less private and more accessible for the law enforcement officials through databases of personal information and thereby constricting the private space. With the increase in attacks, the need for increased scrutiny on the digital sphere due to online terrorist recruitment has curtailed public freedom in the digital sphere. There is considerable debate on the merits of surrendering privacy rights and civil liberties for greater public safety. Digital surveillance has impacted the lives of those being watched in many ways, especially in the way and manner their personal information is used by state authorities (Orji, 2016).

Certain efforts of the government have been widely criticized in terms of surveillance. Peace Brigades International (2012) stated in relation to human rights defenders (HRDs) in Kenya that "incidences of surveillance by state and non-state actors have been reported. Offices

have been raided or burgled and computers hacked, and several organizations suspected that their phones were being tapped. Human Rights Watch (2013) warned of the rising attacks on Human Rights Defenders. In July 2015, it was revealed that agents of the Kenyan intelligence services had contacted intrusion malware company Hacking Team to ask them to shut down a critical blog 'Kahawa Tungu' as a 'proof of concept' for their surveillance tools (Global Privacy Network, 2016). The combination of these trends raises serious concerns about the government's potential use of surveillance tools to further repress on civil society and human rights activists (Nafulka, 2015), especially in the context of the 'war on terror,' which the government has used as a legitimizing narrative to justify serious human rights violations. Some critiques have pointed out the rise of a repressive society that brings in the old reminiscence of a totalitarian state such as of an emerging Orwellian society where personal privacy is a casualty of the counter terrorism campaign.

Concluding Remarks: Balancing the Digital surveillance and Privacy Discourse

Digital surveillance encompasses the same challenges encountered in the past surveillance contexts (Owellian state or the panopticon) such as infringements on the right to expression, movement and privacy. The novelty in digital surveillance is the use of new technologies in surveillance shaped by the fast changing dynamics of technological innovations. This article raised important themes on the nature of the internet and how digitized platforms were used by state and non-state actors and how national security, surveillance and censorship are conceptualized and defined. Further, the article discussed on how countries like Kenya combat or counter pre-emptive threats to national security and faces the challenge on the right to privacy.

In the name of state counter terrorism efforts, various fundamental rights can be at stake. Like many other countries plagued by terrorism, the Kenyan context face similar human rights violations. As emphasized by human rights defenders, these rights include the right to life (extrajudicial killings or targeted killings), liberty (arbitrary detention), profiling of individuals (ethnic, racial), freedom of speech and association, and the right to privacy (Peace Brigade International, 2012). Authors such as Culnan (1993) and Lim (2000 as cited in Chung, 2002) have privacy in the light of the degree of control of information by people. According to Culnan (1993), privacy exists only when the usage, circulation and release of individual information can be controlled. Lim (2000 as cited in Chung, 2002) expressed the invasions on privacy due to the inability of individuals in maintaining control over their private information and usage. Such invasions become a necessity in counter terrorism efforts where the search for terrorist involves an in-depth analysis on personal data and information, which sometimes go beyond national borders. Occasionally, this may incorporate the assistance of third parties with the inflow and outflow of extensive amounts of information (Human Rights Council, 2012). For example, in cases such as of Ms. Amina Mwaiz Muange, a Kenyan citizen who was arrested in India, was linked to ISIS. Information from security agencies of three countries – Abu Dhabi, Kenyan and India, facilitated in arresting her (Kemei, 2015). Also was the case Hassan Abdi Dhuhulow - a Norwegian of Somali descent, who had been involved in the Westgate attack in Kenya. Several countries have been involved in investigating the Westgate terrorist attack, and the identification of Hassan Abdi mainly incorporated security agencies such as Norway’s Police Security Services, US Federal Bureau of Investigation and the Kenyan Authorities (The Local, 2015).

Investigation into terror suspects or persons sympathetic to terrorist organization involves the need for in-depth understanding of the person and his or her involvement. This entails in-depth searches on data bases and related data sets, which is described as Meta data. Meta data goes beyond the actual conversations between people to the details of the caller or the source itself rather than the content. This assist in understanding the model of social relationships involved in the call process, the origin on the call to whether the call was picked up. If it is an image, where the image was created or originated, who created it and the device in which it was created can be traced and kept in databases sometimes for years of investigations (Coscarelli, 2013). The many new possibilities and difficulties encountered in investigations associated to metadata, involves a new area of lawful interceptions and surveillance, which often comes under frequent reviews and critiques (Branch, 2014)

With these advancement of technologies, the Report of the Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, highlighted that technological advancements have led to advanced instruments of control, wherein privacy too is put into task. This involves the use of arbitrary searches in databases, forming of databases and lists, profiling of potential suspects and the formations of databases and datasets to calculate probability of individuals to carry out suspicious activities, mainly with the aim of a deterrence strategy (Human Rights Council, 2009). Digitalization of surveillance through data policies can directly impact the freedom of movement through digitalizing datasets. This includes restriction of mobility through the creation of watch list, being in the police radar, excessive data collection, sharing of biometrics, information from intrusive scanning devices. These data are shared among different intelligence networks and profiles being developed to aid countering cyber-crimes and terrorism. Therefore, in the face of national security, the right to privacy is not an absolute right and is at stake amidst the state of emergency threatening national security. In the fight against terrorism, the need for systematic individual data propels authorities to plug data into databases to profile particular terrorists or design particular typologies (Theohary and Rollins, 2011). This may also include bans on particular sites. As Human Rights Council Report (2016) notes, 'that bans on the operation of certain sites should not be generic but content-specific; and no site or information dissemination system should be prohibited from publishing material solely on the basis that it may be critical of the government or the social system espoused by the government. Independent judicial recourse must be available.

Hence, surveillance in the namesake of national security often have a powerful effect on privacy. There is an inverse relationship that, if surveillance increases, other rights such as privacy decreases, hence revealing a clash between the two rights. A main factor in this clash, is the aspect of the right to privacy and other rights associated to the right to privacy itself. For, privacy acts as a basis for other rights such as the freedom of association, freedom of expression and freedom of movement (Human Rights Council, 2009). The right to freedom of association and assembly are often threatened by the use of surveillance, as an increase in surveillance powers could lead to a 'function creep'(Scheinin, 2013:14) due to the labeling of particular groups or organizations as terrorist organizations, where the government use surveillance powers which was initially given only to fight terrorism. In Kenya, the case of the secessionist group, Mombasa Republican Council brought in wide criticism on the government surveillance capacity for labelling organizations as terrorist organizations (Boru, 2013). Further, the Kenyan opposition, the Coalition for Reform and Democracy (CORD) filed a suit (Petition No. 628 & 630 of 2014)

which challenged the Security Amendment Law 2014 that focused on a strong surveillance role under the national security organs (Goitam, 2014).

Despite the existing legislative clash between privacy and surveillance policies, many governments focus on surveillance as a main strategy for countering terrorism. One main impact is in data profiling through the use of data bases, supervision of internet traffic and use of data sets. However as the Report of the Special Rapporteur highlights, there are cases in which surveillance have resulted in wrongful convictions (Popp & Poindexter, 2006). For example, transnational terrorist networks such as the al-Shabaab operate worldwide. The data of these terrorist members and groups associated with their activities can be easily mixed with data pertaining to people who are not terrorists or involved in the group. In such cases, it becomes difficult to differentiate the ones who are involved from the ones who are not involved, raising the question if the government needs access to this data, they should also ascertain some way to protect the privacy of those who are not involved in the terrorist group (Ibid, 2006). Therefore, surveillance may work to a particular point, but may affect large number of people who are innocent creating surveillance communities also known as 'suspect communities' such as young Muslim youth in Eastleigh or Muslims in Muslim dominated marginalized regions (Badurdeen, 2017). In this regard, Hammarberg (2008), identified the 'false positives' of classifying innocent individuals as suspects or 'false negatives' not identifying the real terrorist or the criminal from very large datasets, missing the point of capturing rare incidents of terrorism from a deterrence perspective.

The need for consistency on internet privacy protection by states is important. This will not only boost electronic commerce but also for national and international security countering cyber-crimes and online aided terrorist activities or cyber terrorism. This necessitates states on agreeing privacy or data protection laws that could be applied across the Internet. Some international and national privacy frameworks have converged to form core basic principles on privacy (Siserman, 2013). An acclaimed guideline originates from the Organisation for Economic Co-operation and Development (OECD) 2013 Protection of Privacy and Trans border Flows of Personal Data. The guideline focuses on collection limitation on personal data, lawful and fair means in obtaining data and where relevant the need to obtain consent of the data subject. The data quality should be accurate, relevant and timely. The purpose of data gathering should be specified. Disclosure of the personal data should authorized by law. Personal data should be protected by reasonable security safeguards. Need for openness with regard to personal data and the right to obtain information about personal data held by others (authorities). Further, the need to be accountable of the data gathered. Principles similar to this guideline also exists in the International Principles on the Application of Human Rights to Communication Surveillance (2013). Thirteen principles were enshrined in this guideline which included aspects such as legality, legitimate aim, necessity, adequacy, proportionality, competency of judicial authorities, the due process, user notifications, transparency, public oversight, integrity communications and systems, safeguards for international cooperation and safeguards against illegitimate access. However, some of the principles had been critiqued on grounds on limiting chances to apprehend criminals or terror suspects, mainly in countries which are vulnerable to terrorist attacks (Media Policy and Democracy Project, 2015).

However, such consistency is not always followed or has been relaxed in contexts such as terrorism, where information needs to be gathered quickly with regard to national security. In these contexts, law enforcement officials have been reluctant to follow such guidelines and in some aspects mandated by state repressive laws on a stronger surveillance role (Human Rights Council, 2016). The two main legislations in support of countering terrorism in Kenya - Prevention of Terrorism Act 2012 and the Security Law Amendment Act, 2014 attest to this fact. In counter terrorism efforts mainly in the use of the Internet for terrorist activities, surveillance policies are usually at deadlock with privacy. In many instances, privacy is neglected within the need for increased surveillance measures to detect potential terrorists, such as the context which followed immediately after the Westgate terrorist attack in Kenya. The magnitude of the impact with more than sixty individuals killed mainly foreigners, pressurized the government locally and internationally to bring the perpetrators accountable. In such instances, where the public point fingers at the law enforcement officials on issues regarding breach of security, pressurizes officials concerned to go into depths on investigation, in many instances infringing the rights such as privacy of individuals concerned. Herein, the violation of privacy rights have repercussions as it does violate other interrelated human rights. Nevertheless, looking from another facet, without countering terrorism one of the most fundamental rights – the right to security and safety linked to the right to life may be breached. Thus, in examining each right, it can be rightfully affirmed that both of them are of utmost importance, highlighting the need to balance the rights in counter terrorism efforts (Siserman, 2013).

There is also the need to agree on the limits posed on the right to privacy. Despite the complication of the context, such as balancing situations wherein non-derogable rights could conflict such as the right to life may conflict with the right not to be subjected to torture. This necessitates the balancing approach where policy makers and legislators will have to weigh the interest of one right against the other to ensure least derogation of rights. In an attempt to balance a right against national security versus, the policy maker or legislator should utilize empirical evidence in achieving national security. Balancing requires the need to 'justify the derogation of human rights by reference to a demonstrated link between the means (which derogates from the human right) and the end (community safety or national security)' (Golder & William, 2006). This may require attempting the pros and cons in terms on socio-political and economic implications of their proposed decision.

There is an emphasis on reconciling human rights and national security as 'human security legislations' rather than counter terrorism legislations may reveal a focused tendency on peace, human rights and human wellbeing. This might be difficult to achieve, especially with differing contexts among different countries and on how they relate to what is entailed in the aspect of privacy. Further, the emphasis on the concept of proportionality requires policy makers and legislators evaluate alternative means. Successful implementation requires being ready to work with a range of counter-terrorist legislations by investigating options such as fostering meaningful cross-cultural, religious community dialogue or critically reviewing the social and economic effects of their foreign policies, initiating community education (Ibid, 2006).

Finally, digital surveillance is critiqued as being anti-ethical to democratic principles (Monahan, 2010). Social control remains the core of surveillance, where human and technical action is regulated and limited by the state. However, social control may be a necessary function of social

regulation, and how can its enforcement by surveillance technologies be more democratic and empowering for people? Here Monahan (2006) asserts that surveillance systems should be designed and regulated along transparent designs, public involvement and local accountability. This may be easier said than done. For, public involvement is not always easy. In security settings such processes are more state centric and are covert. Hence how do we have public participation to make digital surveillance processes to be democratic and have socially empowering designs? It may not be easy, as surveillance systems manipulates data for the purposes of control and more or less finds it difficult to be transparent. Nevertheless, some form of democratic process can be incorporated, as inviting participation from members of the community to foster learning or design participatory forms of surveillance. While all aspects of digital surveillance cannot result to democratic surveillance, we have the option of moving out of 'marginalizing surveillance' (Monohan 2010). In this case, the marginalization of already marginalized societies such as Muslim communities which have been classified as risk societies, where digital surveillance on particular risk societies can result in double victimization in the name of social control in line with surveillance as governance (Badurdeen, 2017).

References

Agnon, S. Y. (2016). Four Shabaab 'Brides' charged over terror attack plot. Available at: http://intelligencebriefs.com/four-shebaab-brides-charged-over-terror-attack-plot/ (accessed on 2 June 2017).

Anderson, D. M. (2014). *Why Mpeketoni matters: Al-Shabaab and violence in Kenya*. Policy Brief. Norway: NOREF, Norwegian Peacebuilding Resource Centre.

Badurdeen, F.A. (2012). Youth Radicalization in the Coast Province of Kenya, *Africa Peace and Conflict Journal*, 5(1): 53-64. University for Peace Africa Programme, Ethiopia. Available at: http://www.apcj.upeace.org/issues/APCJ_Vol5_1_00i_064_Web.pdf (Accessed on 10 November 2016)

Badurdeen, F. A. (2016). Digital Surveillance in Countering Cyber Terrorism in Kenya: Ethical dilemmas and moral panics. Paper presented at the CODESRIA workshop 'The African State and the Public Cyber-security Service' in Dakar, Senegal on 26 November 2016.

Badurdeen, F. A. (2017 December forthcoming). Surveillance of Muslim Youth and Counter Terrorism in Kenya, in Grasso, M. & Bessant, J. *Governing Youth Politics in the Age of Surveillance*. London: Routledge Publications.

Bloss, W. (2007). Escalating U.S. Police Surveillance after 9/11: An examination of causes and effects. *Surveillance and Society*, 4(3): 208-228.

Boru, A. (2013). Kenya must engage with Mombasa Republican Council. Not demonise it. *Sahan Journal*. Available at: http://sahanjournal.com/kenya-must-engage-with-mrc/#.WX9uL4SGPIU (accessed on 20 March 2017)

Branch, P. (2014). Metadata and the law: what your smart phone really says about you. Available at:
http://theconversation.com/metadata-and-the-law-what-your-smartphone-really-says-about-you-23827 (accessed on 23 July 2017)

Chumba, E., Okoth, P. G., Were, E. (2016). Effectiveness of Border Surveillance Strategies in the Management of Transnational Terrorism in Kenya and Somalia. *International Journal of Political Science*, 2(2): 39-53.

Chung, W. (2002). A Snoop at privacy issues on the internet in New Zealand. *University of Auckland, Business Review*, 4(2).

Coscarelli, J. (2013). Metadata can be more revealing than your actual conversations. Available at:
http://theconversation.com/metadata-and-the-law-what-your-smartphone-really-says-about-you-23827 (accessed on 23 July 2017)

Culnan, M. J. (1993). 'How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3): 343-363.

Electronic Frontier Foundation. (2014). Necessary & Proportionate International Principles On the Application Of Human Rights Law To Communications Surveillance: Background and Supporting International Legal Analysis May 2014. Available at: www.eff.org. (Accessed June 5 2017)

Gandy, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo.: Westview.

Graham, K. & Felicio, T. (2006). *Regional Security and Global Governance: A study of interactions between regional agencies and the UN Security Council with a proposal for a Regional-Global Security Mechanism*. Brussels: VubPress.

Graham, S and D. Wood. (2003). Digitizing surveillance: categorization, space and inequality, *Critical Social Policy*, 20(2), 227-248.

Global Privacy Network. (2016). State of Surveillance: Kenya. Available at:
https://www.privacyinternational.org/node/735 (Accessed on 12 November 2016)

Goitom, H. (2014). Kenya: Security Laws (Amendment) Bill Enacted. Global Legal Monitor. Available at:
http://loc.gov/law/foreign-news/article/kenya-security-laws-amendment-bill-enacted/ (accessed on 21 June 2017)

Golder, B. & William, G. (2006). Balancing national security and human rights: Assessing the legal response of common law nations to the threat of terrorism. *Journal of Comparative Policy Analysis*, 8(1): 43-62.

Hammarberg, T. (2008). Protecting the right to privacy in the fight against terrorism. Available at:
http://www.un.org/en/sc/ctc/specialmeetings/2011/docs/commissioner-rights-protectingprivacy.pdf (accessed on 5 May 2017)

Hier, S. P. (2003). Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance and Society*, 1(3): 399-411.

Human Rights Council. (2009). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. Available at:
http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed on 12 May 2017)

Human Rights Council. (2012). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson. Available at:
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-14_en.pdf (accessed on 12 May 2017)

Human Rights Council. (2016). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Available at:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0ahUKEwiu4de_n7bVAhWMAMAKHfL_ArIQFghOMAY&url=http%3A%2F%2Fwww.ohchr.org%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession31%2FDocuments%2FA.HRC.31.65_AUV.docx&usg=AFQjCNGwv_orQdyH6ot-tCxqYPT5MuvFog (accessed on 12 May 2017)

Human Rights Council. (2017). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Available at:
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_61_EN.docx (accessed on 12 May 2017)

Human Rights Watch. (2014). Kenya: Security Bill Tramples Basic Rights: Law makers should reject amendments. Available at:
https://www.hrw.org/news/2014/12/13/kenya-security-bill-tramples-basic-rights (Accessed on 20 November 2016)

International Principles on the Application of Human Rights to Communication Surveillance (2013). Available at:
https://necessaryandproportionate.org/about (accessed on 12 March 2017)

Introna, L. D. and Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance and Society*, 2 (1): 177-198.

Jones, R. (2001). Digital ruel: punishment, control and technology. *Punishment and Society*, 2(1): 5-22.

Juma, Y. (2015). 3 alleged Daesh "Jihadi brides" appear in Kenya court. http://aa.com.tr/en/politics/3-alleged-daesh-jihadi-brides-appear-in-kenya-court/62350 https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=Cyber+Crime+Reports+Link+Four+Kenyan+Women+To+International+Terrorists&* (Accessed on 12 January 2017)

Kemei, A. K. (2015). Suspected Kenyan ISIS sympathizer arrested. Available at: https://citizentv.co.ke/news/suspected-kenyan-isis-sympathizer-arrested-109082/ (accessed on 20 March 2017)

Khader, M. (2016). *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference.

Kuner, C. (2013). *Transborder data flow regulation and data privacy law*. Oxford: Oxford University Press.

Lianos, M. (2003). Social Control after Foucault. *Surveillance & Society* 1(3): 412-430 http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf (Accessed on 16 October 2016)

Lianos, M. and Douglas, M. (2000). Dangerization and the End of Deviance: *The Institutional Environment, British Journal of Criminology* 40(3): 264-278.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press and Malden MA: Blackwell.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (2007). *Surveillance Studies: An Overview.* Cambridge: Polity Press.

Mahmoud, F. Z. M. & Zeki, A. M. (2016). Edward Snowden Disclosures turns the fears of surveillance into reality: The impact and transformation in Information Security. *Journal of Theoretical and Applied Information Technology*, 83(2):173-179.

Marx, G. T. (2002). What's New about the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society* 1(1): 9-29. http://www.surveillance-and-society.org (Accessed on 16 October 2016)

Media Policy and Democracy Project. (2015). An analysis of the communications surveillance legislative framework in South Africa. Available at: http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (accessed on 14 May 2017).

Milanovic, M. (2015). Human Right treaties and foreign surveillance: Privacy in the digital age. *Harvard International Law Journal,* 56(1): 81-146.

Miller, E. (2013). Al-Shabaab attack on Westgate Mall in Kenya: Background Report. Global Terrorism Database. University of Maryland, USA. Available at: http://www.start.umd.edu/sites/default/files/publications/local_attachments/STARTBackgroundReport_alShabaabKenya_Sept2013.pdf

Mkongo, M. (2015) Four 'Jihadi brides' granted bail after 2 years in remand http://www.the-star.co.ke/news/2017/01/27/four-jihadi-brides-granted-bail-after-2-years-in-remand_c1495247 (Accessed on 12 January 2017)

Mohochi, S. M. (2011). Preventive Counter Terrorism Action: Case Study of Kenya. SSRN Electronic Journal available at: https://www.researchgate.net/publication/228214415_'Preventive_Counter_Terrorism_Action'_Case_Study_of_Kenya (Accessed on 20 November 2016)

Monahan, T. (2006). Questioning Surveillance and Security, In (ed.). T. Monahan, *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.

Monahan, T. (2010). Surveillance in the Times of Insecurity. New Jersey: Rutgers University Press.

Mwazighe, C. L. (2012). Legal Responses to Terrorism: Case Study of the Republic of Kenya. Master Thesis. Postgraduate Naval School, Monterey, CA.

Nanfulka, J. (2015). Is Kenya putting the chill on internet freedoms? Retrieved: http://cipesa.org/2015/03/is-kenya-putting-the-chill-on-internet-freedoms/ Accessed on 20 February 2017

OECD (2013). Protection of Privacy and Trans border flows of Personal Data. Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed on June 5 2017).

O'Harrow, R. (2006). *No Place to Hide: Behind the scenes of our emerging surveillance society.* Free Press.

Oriji, U. J. (2014). Deterring Cyber-terrorism in the Global Information Society: A Case for the Collective Responsibility of States, *Defence Against Terrorism Review,* 6(1): 32-34.

Orji, U. J. (2016). Balancing State Digital Surveillance Powers and the Right to Privacy in Africa's Information Society. Lecture presented at the CODESRIA 2016 Democratic Governance Institute: The African State and Public Cyber-Security Service on 30 November 2016. Dakar: CODESRIA.

Palmer, D., Warren, I. & Miller, P. (2014). Privacy, Dataveillance, and Crime Prevention, in Reda, A., Rokne, J. *Encyclopedia of Social Network Analysis and* Mining (pp.1353-1362).

Peace Brigade International (2012). *An assessment of the feasibility and effectiveness of protective accompaniment in Kenya.* London: Peace Brigade International.
(accessed 11 June 2017)

Popp, R. & Poindexter, J. (2006). Countering Terrorism through information and privacy protection technologies. *IEEE Security and Privacy,* 4(6): 18-27.

Rachel, B. (2015). Cyber Crime Reports Link Four Kenyan Women To International Terrorists http://intelligencebriefs.com/cyber-crime-reports-link-four-kenyan-women-to-international-terrorists/ (Accessed on 12 January 2017)

Ramah, R. (2014). Kenya to Launch New Hi-Tech Surveillance System to Tame Insecurity. All Africa website:
http://allafrica.com/stories/201405230168.html (Accessed on 20 November 2016)

Rispoli, M. (2015). Kenyans face new privacy threats as state expands surveillance powers. Retrieved:
https://www.privacyinternational.org/node/99
Accessed on 20 February 2017

Sheinin, M. (2013). LIBI Committee Inquiry on Electronic mass surveillance of EU citizens. Available at:
https://iow.eui.eu/wp-content/uploads/sites/19/2015/04/141013-LIBE-Scheinin-Supporting-Docs.pdf (accessed 11 June 2017)

Simcox, R. (2015). *Surveillance after Snowden: Effective Espionage in an Age of Transparency*. London: Henry Jackson Society.

Siserman, C. (2013). A Global perspective on the protection of privacy and related human rights in countering the use of internet for terrorist purposes. *Masaryk University Journal of Law and Technology*, 7(2): 401-421.

Sparrow, E. (2014). Digital Surveillance in Global Information Society Watch 2014: Communication Surveillance in the Digital Age. Available online:
https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf
(Accessed on 12 November 2016)

The Constitution of Kenya (2010). Available at:
http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010 (accessed on 20 June 2017).

The Local (2015). Norwegian was terrorist in Kenya Mall Attack. Available at:

https://www.thelocal.no/20150904/norwegian-was-terrorist-in-westgate-attack (accessed on 5 June 2017)

The Security Laws Amendment Act 2014. Available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf (Accessed on 16 November 2016)

Theohary, C. A. & Rollins, J. (2011). *Terrorist use of the internet. Information operations in Cyberspace.* Philadelphia: Diane Publishing.

United Nations Office on Drugs and Crime (2012). The use of the internet for terrorist purposes. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed on June 5 2017)

Von Behr, I., Reding, A., Edwards, C. & Gribbon, L. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism. Rand Publications. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf (accessed on 22 June 2017).

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: United States Institute of Peace Press.

Warren, S. D. & Brandeis, L. D. (1980). The Right to Privacy. *Harvard Law Review*, 4(5): 193-220.