DIGITAL SURVEILLANCE AND PRIVACY CONCERNS IN THE COUNTER-TERRORISM DISCOURSE IN KENYA: POLICY IMPLICATIONS

FATHIMA AZMIYA BADURDEEN
TECHNICAL UNIVERSITY OF MOMBASA, KENYA
PRESENTATION AT THE CPR SOUTH 2017, YANGOON, MYANMAR, 31 AUGUST 2017
Introduction

- This policy brief explores the use of digital surveillance in countering terrorism and its infringement on privacy rights.
- Using Kenya as a case study, the policy brief expounds on digital surveillance amidst the complexities of balancing the two rights: the right to security and the right to privacy.
- The country grapples with the threat of terrorism with new waves of online propaganda and recruitment by terrorist organizations such as the al-Shabaab and the ISIS, necessitating digital surveillance as means to counter terrorism.
- The clashing of the two rights have been at the epitome in discussions centered on digital surveillance in the counter terrorism discourse. For, various counter-terrorism strategies online, necessitates the encroaching into the privacy context of particular individuals, raising various criticisms from human right organizations, on human rights violations mainly with regard to the right to privacy.
To explore on the context of the state to carry out digital surveillance programmes to counter terrorism without infringing the right to privacy.
‘Digital’ within the ‘new surveillance’

- 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. This provides immense potential for pervasive surveillance due to digitization that facilitates a change in power, intensity and scope of surveillance (Graham & Wood, 2003).
‘Digital’ within the ‘new surveillance’ – Cont.

- Digital surveillance encompasses the same challenges encountered in the past surveillance contexts (Owellian state or the panopticon) – digital panopticon?

Source: The Deep zone website

Source: Ground zero website
The Need for Digital Surveillance as a counterterrorism strategy

- Increase in terrorist acts (geographic factors, marginalized pockets of Muslims, availability of youth, appealing religious extremist ideologies, presence of recruiters/al-Shabaab sympathizers, trigger factors such as KDF entry into Somalia, a...
The Need for Digital Surveillance as a counterterrorism strategy – Cont.

Terrorism incidents have escalated since 2011.

In 2012, a year after Kenya’s incursion into Somalia, the number of attacks was almost double that of 2011.

Source: Global Terrorism Database
Internet Use in Kenya

- Internet Users in Kenya (2016*) 21,248,977
- Share of Kenya Population: 45% (penetration)
- Total Population: 47,251,449
- Share of World Internet Users: 0.6%
Increased use of the online technology by terrorist groups such as al-Shabaab & ISIS (spread of the internet, advancement of technology, increase in direct/physical surveillance, anonymity, fast pace, self-radicalization, youth appeal in the technology/attractiveness of the online techniques).

Source: Jihadology website
Increased use of the online technology by terrorist groups – Cont.
The increase in internet aided terrorist acts
Counterterrorism measures and its impact on surveillance

Adoption of surveillance was to keep pace with technology and pursue crimes on a global scale across transnational linkages.

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.
Adoption of surveillance was to keep pace with technology and pursue crimes on a global scale across transnational linkages – Cont.

- 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.
Privacy within the Kenyan Digital Surveillance discourse

- Peace Brigades International (2012) stated in relation to human rights defenders (HRDs) in Kenya that incidences of surveillance by state and non-state actors had been reported.
- Offices have been raided or burgled and computers hacked, and several organizations suspected that their phones were being tapped.
- 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).
Need for Legitimacy and Proportionality

- 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, especially in the context of the 'war on terror,' which the government used as a **legitimizing narrative to justify serious human rights violations**.

- In some cases the **legitimacy and proportionality** in digital surveillances been questioned, lacking empirical evidence in decision-making.

- The **timeliness** of the need for such surveillance with regard to national security being used as an argument for the need for prompt interventions in mitigating the threat of terrorism.
Privacy as a basis for other rights

- In the name of state counter-terrorism efforts, various fundamental rights are at stake.
- Among other rights – the right to privacy.
- 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.
- 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 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).
Need for a universal definition on terrorism

- **The need for an universal definition of terrorism:** Without an universally agreed definition of terrorism, there is a danger that States may create broad, overreaching definitions and inadvertently criminalise outside the realm of terrorism. This is of a very high importance in determining how the Internet can be used for terrorism purposes and to which degree the activity on this virtual environment can be legally put under surveillance and controlled.

- There is no comprehensive internationally binding instrument setting binding norms on what is considered appropriate Internet content or how States should regulate Internet-related activity within its territory. In their view, the absence of a universally agreed definition of terrorism presents an ongoing obstacle to any internationally agreed approach to the appropriate regulation of terrorism-related activity over the Internet.
Privacy vs Information sharing

- Lim (2000) expressed the invasion 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).
- Eg: reuse of information, effective oversight mechanisms, transparency and integrity
Digitalizing Datasets

- 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.
**Impact of Data Profiling**

- One main impact is in data profiling through the use of data bases, supervision of internet traffic and use of data sets.

- 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). Eg: ‘suspect communities’
Consistency on Internet Privacy Protection

- 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.
Lack of Consistency

- 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).

Need for empirical evidence

- In an attempt to balance a right against national security versus privacy, 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 of socio-political and economic implications of their proposed decision.
Accountability in Digital Surveillance

- 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.
Conclusion

1. Focus on empirically driven policies rather than hasty decisions
2. Balancing the two rights
3. Definition of terrorism and ‘terrorist acts’
4. Consistency in International Privacy protection - Digital protection regimes
5. Regulation on data gathering and storing, data sharing, e.g.: laws based on legality and proportionality
6. Regulation of secondary use of data – who uses and for what purpose?
7. Regulating data sharing processes – sharing with third parties
8. Oversight mechanism – internal and external
9. Can we look forward for more transparency digital surveillance mechanisms with public participation? The degree of participation?
THANK YOU