IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 21, Issue 7, Ver. VIII (July. 2016) PP 64-72
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

"Right to Privacy and Counter-terrorism in the Digital Age: A Critical Appraisal for Bangladesh"

Md. Abu Bakar Siddique [1] Sharmin Akter[2]

1. *Lecturer, Department of Law, Bangladesh University of Professionals (BUP), Dhaka-1216, Bangladesh.*
2. *Senior Lecturer, Department of Law, Eastern University, Dhaka-1206, Bangladesh.*

ABSTRACT: Modern life is simply impossible without information and communication technology (ICT). The pattern of interaction in ICT is increasing and changing our daily life unprecedentedly. Simultaneously terrorism through on and off digital domain is increasingly posing immense challenges to Bangladesh. Meanwhile technological capabilities of Bangladesh to intercept communications for investigation, forestallment and prosecution acts of terrorism and other serious crime have also been intensified. Hence counter-terrorism ventures by the states have jeopardized many human rights inter alia "right to privacy" of the people irrespective of terror affiliations. This article has endeavored to explore the discourse from legal perspective. It further tries to critically examine the underlying issues to sketch inherent tension between mass digital surveillance and protection of right to privacy. Considering the emerging evidences of terrorism in Bangladesh in digital form, this paper advocates for taking proactive counter terrorism ventures (i.e. digital surveillance) rightly premised on accessible legal regime. It calls for enacting an explicit and detailed laws premised on 'legality and proportionality' principle on right to privacy to strike a proper balance. It concludes that Right to privacy is not adequately mainstreamed due to lack of equal compensatory provision within the newly enacted Cyber Security Act 2015 which necessitates amendment.

KEY WORDS: *Right to Privacy, Counter-Terrorism, Digital Surveillance, Bangladesh.*

I. INTRODUCTION

"We live in a world today where vast Information and Communications Technology (ICT) infrastructures and extensive flows of information have become natural and unquestioned features of modern life. Rapidly growing online services— everything from social media to ecommerce and virtual collaboration—have come to define our day-to-day lives in ways unimaginable just a decade ago" (Hope 2011).

The changing infrastructure of ICT and interaction of our life is inevitably impacting almost every aspect of our society. Digitalization process has brought about this utter shift and added momentum in almost everything we think and execute. In addition to multifaceted uses, Internet technology is often resorted by terrorist groups and their followers for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes (UNODC 2012). Simultaneously, Bangladesh as growing economy 'has been strategically, operationally and tactically challenged by the new techniques and technology of terrorism' (Islam 2008).

The government of Bangladesh is well aware of the terror threat from religious militants and their international associates. For this, apart from legislative amelioration, government has planned to boost up surveillance capacity to get over maximum monitoring control in digital communications (Byron 2015). Furthermore, the targeted surveillance also enables intelligence and law enforcement agencies to monitor the online activity of particular individuals, to penetrate database and cloud facilities, and to capture the information stored on them. Therefore, this pervasive, unpredictable, and rapidly changing growth and incorporation of surveillance measures have jeopardized many human rights issues; most importantly right to privacy. As primary duty bearer Bangladesh government will have to endure this challenge to protect citizens' right to privacy in one hand and at the same time; protect them from clandestine and explicit threat of terrorism.

In this back drop this research finds its rationale to be studied specifically to bring about light on this emerging sophisticated discourse. In the coming decades of the digital age, developing country like Bangladesh will have to undergo with this paradox more rigorously. Therefore, this research would like to seek probable answer for the question that- what are the impinging factors of right to privacy and counter-terrorism measures those should be taken into consideration to create better protection regime that accommodates both the legitimate claims?

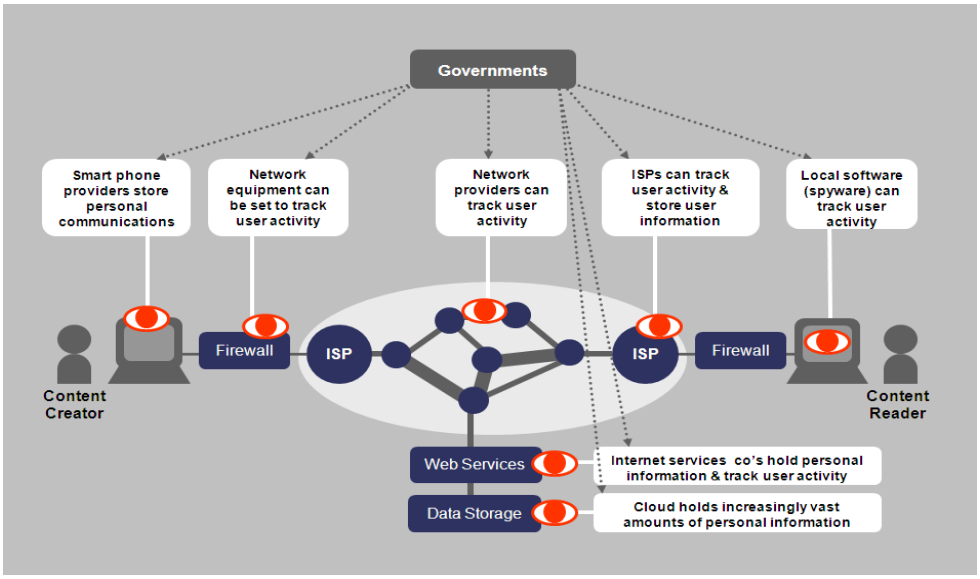
II. METHOD OF THE STUDY

This research has mostly employed qualitative method of study. To analyze the research question the authors have relied upon publicly available data and scholarly contributions from home and abroad scholars on right to privacy and counter-terrorism. Throughout the study an inductive approach is specifically adhered to critically examine the underlying issues (i.e. privacy interface, legal definitions and evidence of terrorism using online in Bangladesh) in order to sketch inherent tension between mass digital surveillance and protection of right to privacy. In the middle of the paper, we have tried to evaluate the extent and necessity of mass digital surveillance to fight against terrorism. Lastly, attempt was made to sort out consequences of breach of privacy and sketch how balancing is possible between these two legitimate claims. The authors humbly recognize the limitations of the paper[1] and have endeavored to overcome those successfully by critical legal analysis.

III. DIGITAL COMMUNICATION AND PRIVACY INTERFACE IN BANGLADESH

'Digital Bangladesh'- has been at the heart of the political manifesto of the current government since the ruling party ascended in the power on 2009. It is undeniable fact that digitalization in every sectors has been geared up since then. From telecommunication to software development, national ID card to driving license, utility bill payments to job application and lastly social networking to beauty aesthetics - everything has been transformed into computer bits and is stored in digital form. According to finance ministry official statement the 'tele-density' in Bangladesh till February 2015 has reached up to 79 percent from 30 in 2009 (Ministry of Finance 2015). The total number of Internet Subscribers has reached 50.707 million at the end of July, 2015 (BTRC 2015). This staggering internet subscriptions is augmented because widespread availability of smart phone and similar devices. Mobile phone operators have substantially contributed to increase internet users as well.

Internet as multiple windows has enabled mass people to interact frequently. Such interactions often requires huge amount of personal information from the end users by the multiple service providers but the major control lies with the government agencies (Hope 2011). However the entire process of communication and digital infrastructure is mostly unknown to the end users. Therefore, the risk drivers of privacy mostly remain tacit to them. To comprehend the question of privacy risk in general the following diagram can be helpful.



Privacy Risk drivers across the ICT value chain[2].

The diagram clearly points that web services, data storage, smart devices, network equipment, Internet Service Providers (ISPs) and Spyware software are under government's monitoring and overseeing purview.

[1] It is mention worthy that the technical know-how of the authors about technology is limited. There can be numerous ways by which privacy can be breached which is not discussed in the paper. The authors acknowledge that it is an attempt to contribute to the existing body of knowledge on this topic mostly from legal perspective.
[2] This diagram is incorporated from (Hope 2011 at page 15).

From content creator to content reader (both are end users), the entire digital communication can be detected and is potentially vulnerable to privacy risk at any stations. These risk drivers are universally similar. Thus, privacy[3] integrity is unquestionably challenged as 'both State and private sector enjoy unprecedented abilities to collect personal data' because of decreasing 'costs of data collection and surveillance' (Froomkin 2000).

A data subject has significantly less control over personal data once information is in a database. Froomkin (2000) in his scholarly article on "The Death of Privacy" further marks that 'privacy enhancing technologies such as encryption provide a limited ability to protect some data and communication from prying eyes and ears', and opined that exclusive privacy is practically impossible today 'unless one lives alone in a cabin in woods'. Since Personal data is produced, stored, circulated and re-used in the ICT value chain by multi-stakeholders; the privacy interface can be drawn in the following ways (Hope 2011 at page 16):

3.1 Private Telecom Sector

Government may demand access to content restrictions, block SMS messaging, call records, caller locations, etc. for "lawful intercept" (real-time monitoring and surveillance, or the provision of analysis and evidence).

3.2 Software/hardware Sector

Software/hardware can be configured to restrict access to certain online content, either at the discretion of the telecommunications network operator or mandated by government. Software/hardware can be designed to enable location-based services (such as mapping or advertising). Such interfering software/hardware can be pre-installed in computers and/or mobile devices. There can be provision of security software to certain customer segments (such as defense, national security, public safety, justice, law enforcement, etc.) by Government. She may prohibit the use of strong forms of encryption or demand that this sector should offer simpler means for encrypted information to be unscrambled.

3.3 Internet services Providers (ISPs)

ISPs can receive demands from governments to remove, block, or filter content, or deactivate individual user accounts, to release personal information, such as emails, web surfing habits, etc. and using filtering software to restrict users' priority searching content.

The privacy risk can be even more immense beyond the above mentioned factors. Digital communication is increasingly under security threat not only by ones' national government rather; often it is argued that, transnational actors[4] are actively involved in privacy invasive activities. Since *prima facie* liability to protect and promote right to privacy requires individual states' affirmative action therefore; this article has tried to focus only on the privacy invading activities mostly committed or patronized by the Bangladesh as individual state.

IV. TERRORISM IN THE REALM OF MASS DIGITAL INFRASTRUCTURES IN BANGLADESH

Terrorism is not myth but reality especially in the post 9/11 incident across the World. However defining terrorism is the most contentious issue in International law. Often it is argued that, the term terrorism is subjectively defined disapproving legitimate protesting right of the alleged terrorists or the political organizations. The pragmatic development of the terrorism definition is therefore not persistent.

4.1. Terrorism defined in International and National law:

Walter et al. (2003) suggests that- "A terrorist act is an act which causes serious interference with or serious disruption of an essential service, facility or system, whether public or private". Hence, it is uncontroversial proposition to Walter et al. (2003 at page 8) that 'the intention of creating terror and fear within the population' is the core ingredient of terrorism definition. In International law, the concept of terrorism had been defined since 1937 to till 2010 in the international instruments[5]. Security Council resolution 1373[6] adopted

[3] Here, privacy is denoted as Informational privacy which is created, flowed and circulated without the exclusive control of its subjects or owners.

[4] Both private organizations and international intelligence agencies for numerous purposes.

[5] 1937 League of Nations Convention for the Prevention and Punishment of Terrorism, 1963 Tokyo Convention on offences and Certain other Acts Committed on Board Aircraft, 1970 The Hague Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1973 New York Convention on the Prevention and Punishment of Crimes Against International Protected Persons, 1979 New York Convention Against the Taking of Hostages, 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1999 New York Convention on the Suppression of Financing of Terrorism, 2005 International Convention For

in 2001 is typically considered the guiding principle for the incorporation of national legislation on terrorism. At present terrorism mostly denotes religious militancy, radicalization and violent extremism by any terrorist individual, group or entity against any state or people. Additionally, with the advent of technology 'terrorism and terrorist threats continue to evolve and manifest themselves differently in different parts of the world' (Brantly and Ubaydi 2014).

In Bangladesh terrorism is not explicitly defined in The Prevention of Terrorism Act 2009[7]. Rather it defines 'terrorist person' in section 2(14) as- who commits any offence under later section 6(1), 10, 11, 12 or 13 of the same Act. The offences listed in these sections have to be committed, conspired, attempted or abated to prejudice the "Sovereignty, Solidarity and Public Safety with the intention to create terror within government and public at large"[8]. Additionally, the proposed Cyber Security Act 2015[9] in the Section 13 defines act of terrorism using cyber technology only by the addition of phrases like "using computer, computer system or computer network" with the existing framework definition given in The Prevention of Terrorism Act 2009**.**

4.2. Terrorism through digital technology in Bangladesh:

Digital security tools, those are developed for the promotion of human rights, often resorted in terrorist activities across the world. For instances, with the increasing 'sophistication of geo-mapping capabilities have heightened terrorists' ability to plan operations with a better understanding of local terrain and its tactical advantages and disadvantages' (Brantly and Ubaydi 2014). To be sure, the nexus between terrorists and criminals has greatly been facilitated by the advent and misuse of ICT and easy access to weapons. The internet has become a fertile breeding ground of terrorist activities. Often it is alleged that there is increasing trend of subversive use of internet to spread and finance act of terrorism by organized criminal entities which also includes use of social media in Bangladesh (Momen 2014). Recruiting 'the young radicals come from affluent backgrounds and also with liberal education', which is opposed to traditional 'Madarssa-educated recruits' of the recent past (Bhattacharjee 2015), is completely a new sign in digital terrorism in Bangladesh.

Hence despite having legislations on terrorism[10]; the 'secular and nationalist foundations of moderate Bangladesh are being undermined by a culture of political violence and the rise of Islamist extremists' (Gohel 2014). Gohel (2014) further marks that Bangladesh had endured 'a wave of violent radicalization during the 1999-2005 period'. Since then, the list of active Terrorist and Extremist Groups in Bangladesh is not more than six[11]. However, most recent emergence of groups like Ansarullah Bangla Team (ABT) illustrates one attack on the minority community in 2012 was planned on Facebook that a new generation of violent extremists; using digital technology for collecting, spreading and getting empathy for their form of terrorist activities, are potentially posing enormous security threat for Bangladesh. Moreover, The ABT has acknowledged the recent killings of four bloggers and online activists mostly because of their role against religious fundamentalism in Bangladesh (Mullen 2015). Consequently, as in other countries, the Internet is increasingly becoming their lifeblood, enabling extremists to spread their doctrine and establishing clandestine networks (Gohel 2014). This concern is being highlighted by the fact that European nationals of Bangladeshi origin are travelling to fight with Al-Qaeda affiliates in Syria. Gohel (2014) also asserts that the 'proliferation of this activity raises a number of security concerns because it creates a potential nexus and blow-back between Europe, Bangladesh and Syria'.

The Suppression Of Acts Of Nuclear Terrorism, Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft. See (Walter et al., 11) and <http://www.un.org/en/terrorism/instruments.shtml> accessed on 28 September 2015.

[6] This resolution along with resolution no 1267 has also been mentioned in the section 20(Ka) of the Terrorism Prevention Act 2009 of Bangladesh. See footnote 9.

[7] This act is amended in 2013 specially focusing on terror financing. The act is available in Bangla version at: http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1009 accessed on 26 September 2015.

[8] *Ibid* at section 6(1) (a). The act is enacted in Bengali and translated unofficially by the authors.

[9] The proposed act is yet to be passed and still it is in consultation stage for multi-stakeholder dialogue. It is drafted in Bengali and the authors have tried to translate in English by their own. <http://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/9e151cd8_72a6_4254_88cb_a6aa336e41f1/Cyber%20Security%20Act%20-%20Nikosh%20%2823.06.15%29%20%281%29.pdf> accessed on September 10, 2015

[10] *Supra note* 9 and 11.

[11] The list is provided in the Institute for Conflict Management official website. It is available at <http://www.satp.org/satporgtp/countries/bangladesh/terroristoutfits/index.html> accessed on September 12, 2015

Bangladesh's radical groups are themselves very active in the cyber world. They use the Internet not only for 'propaganda and to garner support but also as a medium of communication so as to share news about their activities' (Bhattacharjee 2015). Additionally, Internet is providing a platform for like-minded people to meet, exchange ideas and establish offline contacts. Bhattachargee (2015) opines that there have cases when radicals have used social media to instigate realtime violence. For example, one attack on the minority community in 2012 was planned on Facebook.

V. COUNTER-TERRORISM AND MASS DIGITAL SURVEILLANCE

The nexus between terrorist networks, non-state actors and trans-national criminals pose newer challenges to States apparatus and the traditional lines of national defense. Innovative and well-coordinated efforts are therefore mandatory from every corner of society. Encountering terrorism entails multi-layered strategy along with traditional responses to criminal activities. Most of the security analysts have categorized counter-terrorism from different perspectives. Crelinsten (2014) categorized these approaches can be- 'Coercive Counterterrorism', 'Proactive counterterrorism' and 'Persuasive Counterterrorism'. According to his contention these approaches have different dimensions and aspects; these are briefly discussed below-

5.1 Coercive Counterterrorism:

Coercive counterterrorism relies on the state's monopoly on the use of violence, (i.e. the exercise of hard power). This lies exclusively with the state jurisdiction. State violence to counter act with terrorism through traditional means falls in the 'Criminal Justice Model' and 'War Model'. Crelinsten (2014) argues that strict limits should be placed on who can be subjected to state violence. These restrictions form the basis of the legitimacy bestowed upon the state by the rule of law, whether national or international (Crelinsten 2014).

5.2 Persuasive Counterterrorism:

This approach patrons the penetration of the root causes of terrorism committed either by digital domain or traditional means. Such approach enables government, who has access to the data on terrorists, not only to detect the plot the movements, actions, and financial activities of suspects, but also to design new techniques for detecting terrorism and identifying suspects. However, Crelinsten (2014) cautioned about the probable danger in this method is that the government or others will attempt to use 'the ability to construct personal profiles in order to predict dangerous or antisocial activities before they happen'.

5.3 Proactive counterterrorism:

Proactive counterterrorism aims to prevent terrorism before it happens. In the area of intelligence, 'it means widening surveillance nets, the identification of dangerous classes of people, increased use of profiling, increasing focus on radicalization to violence' (Schmid 2013). Pedahzur and Ranstorp quoted in (Crelinsten 2014) further elaborates that-

> "[T]hrough intrusive techniques involving surveillance, wiretapping, eavesdropping and other means of spy camera, agents of all stripes have devoted their energies more and more to stopping terrorists before they act and thwarting terrorist plots before they develop too far".

This approach is mostly undertaken by many states as it has enormous avenues to desist the terrorists' ultimate plan as well as targets. It is helpful to prevent harm before it takes places.

5.4 Digital Surveillance:

The digital surveillance has been derived from the 'The Intelligence Model' which emanates from 'proactive counter terrorism' approach. The intelligence function is an important element in any counterterrorist effort. In proactive security intelligence, information is not gathered for evidentiary purposes but for intelligence purposes (Pedahzur and Ranstorp 2001). Targeted surveillance also enables intelligence and law enforcement agencies to monitor the online activity of particular individuals, to penetrate database and cloud facilities, and to capture the information stored on them. An increasing number of states are making use of "malware systems that can be used to infiltrate an individuals' computer or smartphone, to override its settings and to monitor its activity and this forms of surveillance provide a mosaic data from multiple sources" (Emmerson 2014). Emmerson (2014) being a special rapporteur on fundamental freedom and privacy terms proactive counterterrorism through mass digital surveillance is therefore a 'double-edged sword'. According to his observation 'it can nip a burgeoning threat in the bud or destabilize a terrorist network enough so that its operatives cannot move from the planning stage and go operational'. On the other hand, it exposes many to the security initiatives and thereby, jeopardizing their 'right to privacy'.

VI. RIGHT TO PRIVACY VERSUS COUNTER-TERRORISM THROUGH DIGITAL SURVEILLANCE

States with high levels of internet penetration can potentially cut through the edge of the privacy by digital surveillance whenever government is willing to do so.[12] This is possible without any prior suspicion over a specific individual or organization. The special Rapporteur Emmerson (2014) argued that every 'communications of literally every internet user are potentially open for inspection by intelligence and law enforcement which is amount to systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling jurisdiction'.

6.1 Right to Privacy in International and National Instruments:

In general sense, 'Privacy' can be defined as the presumption that individuals should have an 'area of personal autonomous development, interaction and liberty free from state intervention' and 'excessive unsolicited intrusion by other uninvited individuals' including state agencies (UNHRC 2014). Furthermore, in discussing Constitutional right to privacy of America Gormley (1992) adds 'three components: 1) a right to be left alone; 2) a right to autonomous choice regarding intimate matters; and 3) a right to autonomous choice regarding other personal matters' with the contemporary notion of privacy. Hence, core International Human Rights Instruments Universal Declaration of Human Rights (UDHR) and International Convention on Civil and Political Rights (ICCPR) clearly prohibit any kind of breach of privacy right within their Article 12 and in Article 17 respectably –

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".[13]

There is no comprehensive legislation on privacy in our country. We do not even have a specific law on privacy like a lot of other countries. Article 43 of Bangladesh Constitution depicts the protection of home and correspondence-

> "Every citizen shall have the right…. [(a)] to be secured in his home against entry, search and seizure; and b) to the privacy of his correspondence and other means of communication".[14]

It is clearly evident from the plain reading of the Article 43 that digital communication is not exclusive because it is subject to the reasonable restrictions on the ground of state security, public order, public morality or public health. Conversely, ICCPR requires states to provide an articulable and evidence-biased justification for any interference with the right to privacy, whether on an individual or mass scale.

6.2 Consequences of Breach of Right to Privacy:

The phenomena of digital surveillance, security and big data are complex and have significant social impact. Ostensibly, surveillance is used as a necessary strategy to protect citizens but in effect it is an insidious means to control and regulate their everyday interactions. Mallan (2014) argues that any kind of 'surveillance and hyper-securitisation' in a civilized society dominantly override citizens' right to privacy which can significantly affect their life and livelihoods innumerous ways. A thorough survey of Clarke (Cited in Mallan 2014) suggests that 'Danger of privacy breach' through data surveillance can bring impact like 'blacklisting', 'witch hunts', 'ex-ante discrimination and guilt prediction', 'selective advertising', 'inversion of the onus of proof', 'covert operations', 'unknown accusations and accusers' and 'denial of due process' at the individual level.

Clarke (1988) emphasized that for the entire society it can bring 'prevailing climate of suspicion', 'adversarial relationships', 'focus of law enforcement on easily detectable and provable offences', 'inequitable application of the law', 'stultification of originality', 'increased tendency to opt out of the official level of society', 'weakening of society's moral fibre and cohesion' and 'repressive potential for totalitarian government'. Modern Social science invariably acknowledges these potential outputs and confirms that we behave differently when, we know, that we being watched. Moreover, since human rights are indivisible, interdependent, and interrelated breach of 'right to privacy' undeniably jeopardize meaningful realization of

[12] See Section 3 of this paper.

[13] For Both UDHR and ICCPR <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.> and <http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf> accessed on 24 September 2015.

[14] See The Constitution of The Peoples' Republic of Bangladesh. <http://bdlaws.minlaw.gov.bd/sections_detail.php?id=367&sections_id=24591> accessed on 24 September 2015

other human rights as well (Maya 2008). Conversely, breaching right to privacy on the well-founded ground of threat to security by terrorists has legitimate premise. Hence a striking a balance between these two is absolutely needed and it is the most challenging task to be done by any state including Bangladesh.

VII. RECOMMENDATIONS FOR BALANCING 'RIGHT TO PRIVACY' AND PROACTIVE COUNTER-TERRORISM MEASURES

The prevention, suppression and investigation of acts of terrorism is clearly a legitimate aim of state. However, establishing effective mechanisms for identifying potential terrorist threats on and off digital domain is not an easy task to be materialized (Emmerson 2014). Plethora of legal, extra-legal and transnational issues interacting simultaneously problematize the balancing discourse between digital surveillance and right to privacy. Despite this hardship, alternative measures can be adopted to maintain privacy integrity while undertaking digital surveillance in the following ways:

- To prevent arbitrary interferences with the right to privacy 'explicit and detailed laws' premised on 'legality and proportionality'(Emmerson 2014 at page 29) principle can be introduced at earliest possible time. Emmerson points that for this, establishing 'independent prior authorization and/or subsequent independent review' authority for any kind of indiscriminate mass digital surveillance can significantly generate progressive acceptance and cooperation from the part of the citizen. This should be set up through the necessary coordination among executive, legislative and judicial body.
- Setting up 'independent oversight bodies' that are 'adequately resourced and mandated to conduct ex ante[15] review of the use of intrusive surveillance techniques' can significantly eliminate negative notion regarding proactive counter terrorism initiatives of the state.
- Each case of inevitable surveillance measure should pass the test of 'legality, necessity and proportionality' under an 'accessible legal regime' on "case-by-case" basis to prevent arbitrary intrusion to right to privacy[16]. This can serve the legitimate aim of the surveillance agencies as well. Hence, Section 14 of the proposed Cyber Security Act 2015 of Bangladesh providing punishment for breach of privacy only by the private individuals but not by any state organs needs immediate reevaluation before the its' final enactment.
- Applying conventional mechanical/technological tactics including a rich variety of interventions (i.e. trojan horses, viruses, and worms) against terrorist organizations' online resource can be adopted and used as proactive counter terrorism surveillance initiatives (Aly et al. 2014).
- Persuasive counter terrorism[17] 'campaigning' via the interactive Internet can serve two purposes at a time. Properly researched and evidence based campaign in digital domain against terrorism can ameliorate privacy index as it can potentially reduce the need for surveillance measures.
- The construction of a 'counter narratives' on violent radicalization and extremism should be properly circulated in the same digital terrain on mass scale. The central focus of such narratives should be not to malign the terrorists but to engage them by forming non-violent activism and civic participation in online (Aly et al. 2014).
- A holistic international cooperation in the fight against terrorism should not rely solely upon a 'supranational legal order or regime'; rather it should also consider universal preservation of right to privacy within that regime.
- Provision for appropriate compensation in proven case of flagrant violations of individual right to privacy by the state should also be accommodated either in the existing legal regime or future one which is currently missing in proposed Cyber Security Act 2015 of Bangladesh.

VIII. CONCLUSION

According to Slaughter (2004), in a post-Westphalian globalized world, domestic politics is not devoid of dimension of transnational/International cooperation for almost every aspect of our life. Therefore, newer ICT product invented at any corner of the world is replacing the older at home necessitating paradigm shift either in its' application or in its' use to harness maximum utility Slaughter (2004). Hence, right to privacy and counter-terrorism discourse is also under a sheer changing process not only in Bangladesh but also everywhere

[15] i.e. after the incident of breach of right to privacy, if any complaint is lodged that should be reviewed as early as possible by the independent oversight bodies.

[16] Special Rapporteur Emmerson endeavors to sketch the probable boundary of 'legality, necessity and proportionality' test as well as the possible 'accessible legal regime' which can be followed as guiding tool.

[17] See section 4.2 of this paper.

across the world. Meanwhile, Bangladesh progress in digitalization and ICT uses is also staggering speedily. At the same time threat of terrorism using digital technology is trying to pulling back this progress. To encounter this threat, along with traditional measures, Bangladesh should take into account citizen's privacy concern by undertaking legitimate actions accommodating both the claims with due care.

Considering the emerging evidences of terrorism in Bangladesh in digital form, this paper advocates for taking proactive counter terrorism ventures rightly premised on accessible legal regime. It calls for enacting an explicit and detailed laws' premised on 'legality and proportionality' principle on right to privacy to strike a proper balance between both the claims. The paper further emphasized to form an 'independent prior authorization and/or subsequent independent review oversight bodies' that are 'adequately resourced and mandated to evaluate ex ante review of privacy invasive activities. It strongly reiterates the Special Rapporteur Emmerson's proposition that inevitable surveillance measure will have to pass the test of 'legality, necessity and proportionality' under an 'accessible legal regime' on "case-by-case" basis to prevent arbitrary intrusion to right to privacy. Simultaneously, the paper further describes that a rich variety of interventions such as trojan horses, viruses, and worms attack against terrorist organizations' and; 'properly researched and evidence based campaign' in digital domain against terrorism can construct 'counter narratives' which can desist terrorist and decrease the necessity to adopt privacy invasive measures.

Throughout the paper critical legal analysis of national and international regime of this discourse explicitly unveils that, the Bangladesh Proposed Cyber Security Act 2015 seems to lag behind the expectation because Right to privacy is not adequately mainstreamed within it. It concludes that compensatory provision should be incorporated within this legislation in case of any gross, unjust and proven violation of right to privacy committed by the state agencies.

REFERENCES

[1] A. Hope, Dunstan "Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry", *BSR report* (2011): 8.

[2] Aly, Anne, Weimann-Saks, Dana and Weimann, Gabriel, "Making 'Noise' Online: An Analysis of the Say No to Terror Online Campaign", *Perspectives on Terrorism*, 8.5 (2014): 33-47.

[3] Bangladesh Telecommunication Regulatory Commission (BTRC): "Internet Subscribers in Bangladesh July 2015", *BTRC report* (2015) <http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-july-2015>, accessed on August 215.

[4] Bhattacharjee, Joyeeta, "Bangladesh's Web of Jihadi Terror", *The Daily Pioneer*, 24 June 2015<http://www.dailypioneer.com/columnists/oped/bangladeshs-web-of-jihadi-terror.html> accessed on September 10, 2015

[5] Brantly, Aaron and `Ubaydi, Muhammad al-, "Extremist Forums Provide Digital OpSec Training", *Combating Terrorism Center (CTC) Sentinel*: 8.53 (2014): 11. <https://www.ctc.usma.edu/v2/wp-content/uploads/2015/05/CTCSentinel-Vol8Issue53.pdf> accessed on September 15, 2015

[6] Clarke, Roger, "Information Technology and Dataveillance", *COMM. ACM* 31 (1988): 1469-71 <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html> accessed on September 15, 2015

[7] Crelinsten, Ronald, "Perspectives on Counterterrorism: From Stovepipes to a Comprehensive Approach", *Perspectives on Terrorism* 8.1, (2014): 1-14

[8] Emmerson, Ben, "Promotion and Protection of human rights and fundamental freedoms while countering terrorism" *Special Rapporteur report in accordance with General Assembly resolution 68/178 and human rights council resolution 15/15*, October (2014).

[9] Froomkin, A.Michael, "The Death of Privacy?", *Stanford Law Review* 52.5, (2000) also available as "Cyberspace and Privacy: A New Legal Paradigm?" (2000): 1461-1543, <http://www.jstor.org/stable/1229519> accessed on 16 October 2015.

[10] Gohel, Sajjan, "Bangladesh: an Emerging Centre for Terrorism in Asia", *Perspectives on Terrorism* 8.3 (2014): 1-8.

[11] [Gormley, Ken, "One Hundred years of Privacy", *Wisconsin Law Review* (1992): 1335-1340.

[12] Islam, Aynul, "Mapping Terrorism Threats in Bangladesh", *BIISS journal* 29.2, (2008): 153-176.

[13] K. Byron, Reajul, "Bangladesh to purchase modern surveillance equipment", *The Daily Star*, August 03, 2015 <http://www.thedailystar.net/frontpage/govt-buy-new-surveillance-tools-120967>, accessed on August 20, 2015.

[14] Mallan**,** Kerry, "*Everything* You Do: Young Adult Fiction and Surveillance in an Age of Security"**,** *International Research in Children's Literature* 7.1 (2014): 1–17 Edinburgh University Press, DOI: 10.3366/ircl.2014.0110

[15] Maya, Gadzheva, "Privacy in the Age of Transparency: The New Vulnerability of the Individual", *Social Science Computer Review* 26.1 (2008): 60–74.
[16] Ministry of Finance (MoF), "Digital Bangladesh-2015", *Inter-ministerial Evaluation report* (2015) <http://www.mof.gov.bd/en/budget/15_16/digital_bangladesh/Digital-2015%20(Text).pdf> , retrieved on September 10, 2015.
[17] Momen, A.K. Abdul, "Open debate on Terrorism and cross border crime" in connection with the agenda item: Threats to international peace and security", *New York*, 19 December (2014)<https://www.un.int/bangladesh/sites/www.un.int/files/Bangladesh/terrorism_open_debate_19_december_2014_1.pdf> accessed on September 10, 2015
[18] Mullen, Jethro, "Extremists in Bangladesh publish global hit list of bloggers and writers", *CNN Online Report,* September 24, 2015 <http://edition.cnn.com/2015/09/24/asia/bangladesh-bloggers-islamist-hit-list/> accessed on September 13, 2015
[19] Pedahzur, Ami and Ranstorp, Magnus, "A Tertiary Model for Countering Terrorism in Liberal Democracies: The Case of Israel,", *Terrorism and Political Violence* 13.2 (2001): 3-22.
[20] Schmid, Alex P. "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review," *ICCT Research Paper*, International Centre for Counter-Terrorism, The Hague (2013).
[21] Slaughter, Anne-Marie, "A New World Order", Princeton *University Press* (2004).
[22] United Nations Office on Drugs and Crime (UNODC), "The Use of the Internet for Terrorist Purposes", *United Nation*, Vienna (2012): 1.
[23] UN Human Rights Committee, "General comment no.16 para 3" and see: *A/HRC/23/40*, para.22 (2013) and A/HRC/13/37, para. 11 (2014).
[24] Walter, Christian, Vonkey, Silja, Roben, Volker and Schorkopf, Frank (eds.) "Terrorism as Challenge for National and International Law: Security versus Liberty*?*", Berlin, Heidelberg Germany, *Springer Online* (2003).