Surveillance and Democracy in India: Analysing Challenges to Constitutionalism and Rule of Law

P. Arun*

Advancements in digital and communication technologies have brought about changes in the nature of surveillance and this in turn has impacted functioning of democracy. Additionally, surveillance is regarded as a grand narrative, accreted as a cultural entity to reduce fear, insecurity, misgovernance, corruption, and provide access to speedy public service delivery and welfare. In this scenario, in order to exercise democratic rights, people need to interlace themselves with surveillance. However, the construction of such a narative conceals the potential corrosive effect of mass surveillance. This paper aims to explore the changes made in the domain of surveillance to face existential challenges and followed by counter effects of deploying sovereign power on democracy, constitutionalism and rule of law. Further, it will examine the significant changes occurring in legal measures and digital technological mechanisms of surveillance in India.

Keywords: *Surveillance, Democracy, Digital Technology, Democracy, India.*

Major terror attacks in early part of the twenty-first century was identified to be one of the major threats to the Indian State. The responses to it have had profound implications for democracy in India. One of the significant response has been the transformation in the nature of State surveillance; it has been linked to burgeoning global terrorism and the development discourse. Simultaneously, there is an unrelenting expansion and frenetic search for alibis to control ever larger areas of society and people. This paper will restrict itself to an examination of surveillance infrastructure, the legal and legislative framework in place and its implications for democracy in India.

In the first section the paper will map how surveillance has engulfed human lives. Then it moves ahead, to analyse the significant changes that have occurred in legal framwork and technological mechanisms of surveillance in India. The legal measures includes provisions for extraordinary and ordinary situation. The quest for increased surveillience was facilitated by technological innovations in monitoring and data-collection; State is now capble of controlling and monitoring its vast territory and population. The paper examines how profound changes have resulted in concern over the need to strike a balance between 'security' and 'freedom'. Later it specifically analyses the challenges and implications of surveillance on Indian democracy. It is an effort to understand and conceptualise the trajectory of continual reforms, innovations, exponential advances in surveillance techniques.

*P. Arun (arun.solarise@gmail.com) is a Research Scholar in the Department of Political Science, University of Hyderabad.

Politics, legalities and mechanisms of surveillance in Indian State

According to David Lyon (2008) surveillance is the "purposeful, routine, systematic, and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection". Surveillance may be direct, face-to-face or technologically mediated; the latter is growing expeditiously and such pervasive and ambiguous proliferation needs methodological understanding (Lyon, 2007, p.1). Surveillance is a dominant organising practice of late modernity; it is used for varied purposes. "We can appreciate the centrality of surveillance to organizational end epistemological endeavourers if we simply step back and survey how various manifestations of watching have become a central institutional preoccupation" (Haggery & Samatas, 2010, p.3). Also, its varied roles in different conditions result in diverse outcomes.

From time immemorial there have been various techniques to monitor, observe, and control population. However, under the gaze of modern State, these techniques and practices of surveillance have become predominant. During colonialism the existence of colonial State depended on the successful mastering, manipulating, codifying, documenting, controlling, classifying, bounding, reporting, and investigating its subjects (Cohn 1996, p. 3-11), and "information order." As Chirstopher Bayly (1996) argued "without good political and military intelligence the British could never have established their rule in India" (p. 10). Under the post-colonial Indian State, surveillance is used as a legitimate means to protect citizens from terrorist attacks and also to govern distribution of rights and entitlements; this qualitatively differs from the erstwhile colonial surveillance. To accomplish that, the State by virtue of its sovereign power directs mass surveillance by biometric identification, creating population records or census, and even arbitrarily monitoring ubiquitously.

The 9/11 (2001) terrorist attack in US shook the entire world; it led to adopting UNSC Resolution 1373 on September 28, 2001 mandating concerted international effort against global terror networks. Later, attack on Indian Parliament building in New Delhi on December 13, 2001 stirred up the demand within India to enact new anti-terror regimes to counter modern terror and its global networks. The 26/11 (2008) terrorist attacks in Mumbai shook the Indian State and this led to major developments in the use of surveillance technologies (Singh, 2012; Singh, 2014).

During this period, the governemnt of India through series of reforms in anti-terror legal regimes acquired new techniques of surveillance for keeping tabs on electronic footprints of its population. The model legislation for interception of wire, electronic or oral communication (Section 14) followed from Maharashtra Control of Organised Crime Act 1999, which originated to deter organised crime. Its provisions included in the Prevention of Terrorism Act (POTA) 2002 in which interception of communication (Section 36–48) was permitted. While POTA was repealed in 2004, its perilous features of surveilling techniques were maintained by incorporating them in the Unlawful Activities Prevention Act 1967 (UAPA), like those relating to the "interception of telephone and electronic communications" (Section 46) (See Table: 1).

Table 1: Comparison of Anti-terrorism Legislation in India

Item	Terrorism and Disruptive Activities (Prevention) Act, 1987	The prevention of Terrorism Bill, 2000 (Draft Bill as recommended by Law Commission of India)	The prevention of Terrorism Act, 2002	The Unlawful Activities (Prevention) Amendment Act, 2004
Interception of communications				
Interception of Communication in certain cities	No separate provision	No separate provision	Separate chapter 5 containing provisions regarding (1) description of communication meant for interception (2) appointment of competent authority by the Central or State Government for this purpose. (3) authorisation of such interception (4) review of order of interception issued by the competent authority by a review committee (5) duration of an order of interception etc.	No such provisions. However, Section 46 provides the following: Admissibility of evidence collected of communications- "Notwithstanding anything contained in the Indian Evidence Act, 1872 (1 of 1872) or any other law for the time being in force, the evidence collected though the interception of wire, electronic or oral communication under the provisions of the Indian Telegraph Act, 1885 (13 of 1885) or the Information Technology Act, 2000 (21 of 2000) or any other law for the time being in force, shall be

Item	Terrorism and Disruptive Activities (Prevention) Act, 1987	The prevention of Terrorism Bill, 2000 (Draft Bill as recommended by Law Commission of India)	The prevention of Terrorism Act, 2002	The Unlawful Activities (Prevention) Amendment Act, 2004
			(6) description of authority competent to carryout interception (7) interception of communication in emergency situations (8) protection of information collected (9) Admissibility of evidence collected through interception of communications (10) prohibition of interception of communications (11) annual report of interceptions	Admissible as evidence against the accused in the Court during the trail of a case: Provided that the contents or oral communication intercepted or evidence derived there from shall not be received in evidence or otherwise disclosed in any trail, hearing or other proceeding in any court unless each accused has been furnished with a copy of the order of the competent authority under the aforesaid law, under which the interception was directed, not less than ten days before trial, hearing or proceeding: Provided further that the period of ten days may be waived by the judge trying the matter, if he comes to the conclusion that it was not Possible to furnish the accused with such order ten days before the trial, hearing or proceeding and that the accused shall not be prejudiced by the delay in receiving such order."

Source: India. Second Administrative Reforms Commission. (2008). *Combatting Terrorism Protecting By Righteousness,* Eighth Report, p. 167. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/cgg/unpan045484.pdf

With such legal frameworks, the Indian State equipped and empowered itself to intercept, tap and eavesdrop telephonic conversations, scrutinise financial transactions and ban suspicious activities (Singh, 2007 , pp.70-75, 325; Singh, 2012, p.439; Singh, 2014, pp. 42-46).

Concurrently, as can be seen in Table 2, in order to protect and provide safeguards against any potential misuse of interception provisions, POTA contained institution of a review committee [Section 40, 46, 60].

Table 2: Comparison of Anti-terrorism Legislation in India

Sl. No	Item	Terrorism and Disruptive Activities (Prevention) Act, 1987	The prevention of Terrorism Bill, 2000 (Draft Bill as recommended by Law Commission of India)	The prevention of Terrorism Act, 2002	The Unlawful Activities (Prevention) Amendment Act, 2004
	Review Committees				
	Review Committee	No separate provision	Clause 39 provides for setting up of review committees by the Central and State Governments to reivew, at the end of each quarter in a year, cases instituted by them under the Act,	Section 60 provides that the Central and State Governments shall constitute one or more review committees for the purposes of the Act.	Section 37 provides for constitution of one or more Review Committees for purposes of review of an order of the Central Government rejecting an application for denotification of a 'terrorist organsiation'

Source: India. Second Administrative Reforms Commission. (2008). *Combatting Terrorism Protecting By Righteousness,* Eighth Report, p. 168. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/cgg/unpan045484.pdf

However, the Central government failed to set up a Review Committee until several months after the Act came into force. Further, Section 48 of POTA mandated the placing of annual report of interceptions before the Houses of Parliament or the State Legislatures. The report is to give a full account of the number of applications for interception and reasons for their acceptance or rejection. It provides for public scrutiny and was, therefore, a potential check on government arbitrariness. However, in the absence of political will these safeguards were never activated. (Singh, 2007, p.153-154). Unlike POTA, UAPA does not have any provision of Review Committee or legislative review. This which makes actions taken under it opaque and not subject to public scrutiny with hardly any safeguard from potential misuse.

Here, the entire legal framework of "anti-terror laws are on extraordinary procedures, which bring into existence dual systems of criminal justice (ordinary and extraordinary), as they differ in terms of procedures" (Singh, 2007, p.314). In extraordinary law, telephone interceptions can be produced as primary evidence against an accused, which is absent in ordinary law (Singh, 2007, p.70). In the climate of global terrorism the Indian State in order to respond, shaped legal measures through state of exception and appropriated surveillance powers. It should be noted in this context that in India the debate surrounding state of exception was rigorously deliberated by framers in Constituent Assembly; they held divided positions on dilemma between liberty and national security. As of now, the state of exception hold constitutional basis in form of emergency and preventive detention provisions (Thiruvengadam 2010, p. 477-479). Apart from provisions for extraordinary situation, there is an array of normal provisions for normal times.

Beyond terrorism related surveillance, the pre-existing laws governing wiretaps permits the government to intercept information from computers to investigate any offense (Gitenstein, 2009, p.31). Telephone tapping and snooping became a serious concern in the post-emergency era. During the tumultuous period of 1980s and 1990s, there were major scandalous revelations about the involvement of several politicians in snooping. Political snooping even led to the resignation of Ramkrishna Hegde from Chief Ministership of Karnataka in 1988. After allegations by Chandra Shekhar, an enquiry by CBI revealed that there were widespread covert and even illegal snooping between 1984 and 1987. Not only the phones of their political opponents but also of their political allies, Members of Legislative Assembly, State ministers, trade union and religious leaders. (Chawla, 1991). Despite the guidelines given by Supreme Court in *People's Union of Civil Liberties v. Union of India* (1996) to regulate such political snooping, massive violations continued. This is the consequence of a legal regime, which authorises the State to intercept as per the procedure established by law. These include provisions as in s.5 (1) and (2) of the Indian Telegraph Act 1885, Rule 419(A) of the Indian Telegraph Rules 1951, as well as s.69 of the Information Technology Act 2009. Further, "while existing laws primarily relates to interception of calls, CMS (Central Monitoring System) expands surveillance across Meta-Data ... Access, transfer and retention of CDRs (Call Data Records) is weakly defined under the existing laws" (Singh, 2013). It empowers the State to intercept communications on the occurrence of any 'public emergency' or 'public safety', or when it is deemed necessary or expedient to do so in the following instances: in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, and for preventing incitement to the commission of an offence (Gitenstein, 2009; Singh, 2014). Undoubtedly, there is an extensive amount of electronic surveillance in India.

Unlike the United States' Foreign Intelligence Surveillance Court (1978) to regulate surveillance and United Kingdom's Investigatory Powers Tribunal (2008) and Intelligence and Security Committee of Parliament to oversee and examine unlawful surveillance India does not have any of such institutional apparatus. In 1996, People's Union for Civil Liberties (PUCL) judgment, the Supreme Court of India retreated from providing 'prior judicial scrutiny' and declared that it is up to the central government to lay down

'procedural safeguards and precautions' from unlawful surveillance. However, it directed and placed restrictions on the class of bureaucrats who could authorise interception, and ordered the creation of a 'review committee' so that the right to privacy is protected. Besides several allegations of phone tapping by politicians on their rivals, there have been few prominent incidents. Gujarat government's surveillance on a woman architect in 2009 ("Fresh tapes on Gujarat," 2013) and the Radia tapes controversy in 2010, revealed a deep nexus between corporate, politics and interception, (Sharda, 2013), whereas the illegal phone tapping by State agencies in Himachal Pradesh in 2013 (Lal, 2013), and the clash between the two recently bifurcated States (Telengana and Andhra Pradesh) in phone-tapping row in 2015 (Singh, 2015) reaffirmed the same. It does reflect the failure of proper procedural framework to provide safeguards from unlawful surveillance and corrupt uses of power.

Major changes in India came about in the post-26/11 scenario to address challenges regarding national security and terrorism. Major initiatives for data-collection included launching of Central Monitoring System (CMS), National Intelligence Grid (NATGRID), an unmanned aerial vehicle (UAV) Netra, and Network Traffic Analysis (NETRA). It reflects how 'surveilling space' was injected into the 'democratic space' of the Indian territory. Such a massive technological establishment was to remould the Indian State. Minister of State in the Ministry of Home affairs, Kiren Rijiju while answering an unstarred Question in the Rajya Sabha noted that the Government of India launched CMS, which can carry out deep search surveillance including monitor mobiles, Short Message Service (SMS), fax, website visit, social media usage, and much more. (India. Parliament, Rajya Sabha, 2014b) It is carried out without any assurance of a matching legal and procedural framework, because it is held that under ordinary operation of the law, individuals could hide behind the law to avoid prosecution for their illegal behaviour (Austin, 2015).

The 26/11 Mumbai attack exposed several weaknesses in India's intelligence gathering and action networks and therefore NATGRID was launched. Minister of State in the Ministry of Home affairs, Kiren Rijiju while answering an unstarred Question in the Rajya Sabha noted that NATGRID will automate the existing manual processes for collation of Intelligence. It shall leverage information technology to access, collate, analyse, correlate, predict and provide speedy dissemination. It is a technical interface or central facilitation centre, with an integrated facility, which aims to link databases of 21 categories (e.g. travel, income tax, driving licenses, bank account details, immigration records, telephone etc.) (India. Parliament. Rajya Sabha, 2014a). In addition to this, its data would be shared with 11 central agencies (e.g. Central Bureau of Intelligence, Intelligence Bureau (IB), Research and Analysis Wing, National Investigation Agency (NIA) etc.). It is essentially 'dataveillance,' wherein the users' actions or communications are monitored and investigated, through which they can be tracked, monitored, intercepted and traced (Lyon, 2007, p.16; Lyon, 2009, p.50).

In order to facilitate, arguably, efficient delivery of welfare services, the Indian State unveiled biometric marking Unique Identification Number (UID) or Aadhaar card, which contains a standard form of 12-digit identity number. It comprises of interlocking

of technologies and mechanisms that serve a range of desires, including those for control, governance, security and much more. Especially by interlocking biometric card with Intelligence Grid and the National Population Register, the colossal database can be shared with various other intelligence agencies and government departments (Singh, 2014; Singh, 2015a). The pilot project UID commenced to provide universal identity and remove ghost-beneficiaries, now it is being linked with NPR data to find out ghost residents. Such an interlocking and convergence reflects that Indian State is not just concerned about efficient delivery of welfare or providing safety and security, but furthermore to keep a surveilling gaze on its population. In a whole this process reflects Haggerty and Ericson's (2000) conceptualisation of "surveillant assemblage" which describes it as a rhizomatic character of surveillance which brings together the multiple, overlapping governing practices which operates with different capabilities and purposes.

It all commenced under United Progressive Alliance (UPA) regime not through statutory law but with a notification in 2009 (Planning Commission, 2009); two years later an effort was made to give it a statutory backing. However, the Parliamentary Standing Committee on Finance rejected the National Identification Authority of India (NIAI) Bill 2010. The committee pointed out the absence of data protection legislation, dangers and issues like access and misuse of personal information, surveillance, profiling, linking and matching of databases and securing confidentiality of information. Later, the Bharatiya Janata Party (BJP - Indian People's Party) led National Democractic Alliance (NDA) government, on March 2016, passed Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Bill in the Parliament as a Money Bill despite severe furore. It does raise some serious questions as Clause 33 (2) says, "disclosure of information, including identity information or authentication records, made in the interest of national security" which shows an intention to use this data for national security and surveillance. In order to protect blatant misuse, this clause lays out "an oversight committee consisting of the cabinet secretary and the secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology." This committee would act as a channel to review any unlawful surveillance by the government. However, if we look into the legacy of the aforementioned committees we can understand corrupt uses of power.

An even more lethal surveilling mechanism is NETRA, an internet monitoring system capable of keyword-based detection, a monitoring, and pattern-recognition system for packetized data and voice traffic in virtual world ("Govt to launch", 2014). Additionally, Netra is also the name of aerial surveillance. These comprise of uninhabited, remotely controlled UAVs or Drones to keep an eye on suspect activity from a vertical position. In India, there has been an extensive utilisation of lightweight UAVs for public safety and security, patrolling, to manage violent protests, crowd management, police investigation and much more in several cities. Furthermore, it is widely used by civilians for private purpose. In October, 2014 Director General of Civil Aviation (DGCA) banned the usage of drones for civil applications citing safety and security concerns (Government of India. Director General of Civil Aviation, 2014). Later in May, 2016 draft guidelines

for drones were released in which it said Unique Identification Number (UIN) would be issued by DGCA. Every drone would be inscribed with UIN and Radio Frequency identity tag or SIM and also need to obtain UA Operator Permit (UAOP) if operated at or above 200 feet in uncontrolled airspace (Government of India. Director General of Civil Aviation, 2016). It shows that "Indian government has sought to monopolize all powers of surveillance" (Singh, 2014, p.50) by making any electronic surveillance by private agencies and civilians an offence.

In 2013 major revelations by Edward Snowden changed the global discourse of surveillance, it swung the pendulum back to the traditional meaning as being a sinister force having "connotations of surreptitious cloak-and-dagger or undercover investigations into the individual activities" (Lyon, 2007, p.13). His revelations were quite grievous about the scope of National Security Agency surveillance not only on U.S population but also on foreign countries, in which India was ranked fifth.

In recent years the data protection and privacy has fallen afoul with the 'third party' (Solove, 2011) i.e. non-state actors. In 2010, Blackberry was warned by the Indian State to either provide access to security agencies to monitor the information on their services or face ban and finally it had agreed to provide access to partial services. In 2010 Indian government asked Blackberry to provide access to monitor their messenger, internet and enterprise service. The company responded by providing lawful access to BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email, but it denied decoding of its intranet facility in BlackBerry Enterprise Service (Singh, 2012). Similarly, the Apple vs. FBI debate intensified issues regarding privacy and security, and it further widened the issues such as the role of State and non-state actors (corporate companies) in data protection.

In a nutshell, the first decade of the twenty-first century witnessed the Indian State making itself technologically competent to control and monitor its territory and population in the name of security.

"Two sides of a coin": conundrum of 'security' or 'freedom'

According to David Jenkins (2014) several legal changes occurred in a decade which he calls a "long decade" where legal systems evolved in reaction to global terrorism not only in India but around the world. Several scholars have tried to understand the nature of surveillance State, and the conundrum between 'security and freedom'. Jeremy Waldron (2003) strikes a note of caution when he states, *"(w)e must also be sure that the diminution of the liberty will in fact have the desired consequence"* (italics as in the original) (p.208). Reducing liberty consequently increases the power of the State and this might in turn cause harm or diminish liberty in other ways. Instead of trading off liberties for purely symbolic purposes and a consequential gain, there should be assessments about the effectiveness of such trade-offs.

However, Eric Posner and Adrian Vermeule advance a trade-off thesis between security and liberty. They argue that both security and liberty are valuable goods that contribute to individual well-being or welfare, and neither good can simply be maximized without regard to the other. One of the characteristics of emergencies or terrorist attacks is

the defensive measures where the government opts to increase intelligence gathering and monitoring. Also, during such period the executive which is swift and vigorous get the institutional advantages along with their secrecy and decisiveness. In contrast, the judges are at sea and the evolved legal rules seem inapposite and even obstructive possessing limited information and limited expertise (Posner & Vermeule, 2007, pp.15-57; Vermeule, 2014, pp.31-45).

Similarly, Richard Posner (2006) maintains that rights should be modified according to circumstance and that we must find a pragmatic balance between personal liberty and community safety. He finds the direct connection between liberty and security just as there is an automatic direct balance between them- a 'fluid hydraulic balance.' It shifts continually as threats to liberty and safety wax and wane (pp.31-41). According to him, "privacy is the terrorist's best friend" (p.143) therefore, the government has a compelling need to exploit digitization in defence of national security. The dangers of data mining, leakage of information should be prevented through sanctions and other security measures (Posner, 2006, pp.143-145).

The trade-off thesis sees the balance between security and liberty as a zero-sum trade-off. However, Daniel Solove finds this argument as completely flawed and argues that the balance between privacy and security is rarely assessed properly. Instead he argues that the real balance should be between "security measure with oversight" and "regulation and security measure at the sole discretion of executive officials" (Solovo, 2011, pp.33-36).

In the West in general and US in particular the role and responsibility of judiciary in times of counter-terrorism and surveillance is considered to be crucial; it is the guardian of constitutionalism and human rights. Jenkins (2016) argues that the judiciary through judicial review has to protect procedural fairness. In order to play a greater role it needs to counter 'pull of deferentialism,' which erodes the particular responsibility of judges (Scheinin, 2016). In this scenario one of the fundamental problems, that judiciary around the world and particulary in India face is how to calibrate the balance between security and freedom.

In India, the concept of freedom does not merely revolve around providing security from potential terrorist attacks, which were actually addressed by several legislative reforms and introducing technologies of surveillance. Rather, it also involves freedom to access welfare schemes and entitlements, freedom from misgovernance and corruption. With this idea, the grand biometric identification project was initiated. However, such an idea diluted the notion of privacy, because there is a general agreement that there is 'nothing to hide' and that it is a 'false trade-off' of privacy in the name of welfare. It is to this aspect that we will now turn our attention.

Challenges to constitutionalism and rule of law

On February 2, 2016, Indian President Pranab Mukherjee, in his inaugural speech at the Counter Terrorism Conference 2016 in Jaipur said, "terrorism is undoubtedly the single gravest threat that humanity is facing today. Terrorism is a global threat which poses an unprecedented challenge to all nations…important aspect of counter-

terrorism strategy is capacity building to prevent attacks through intelligence collection and collation, development of technological capabilities, raising of special forces and enactment of special laws" (India. Press Information Bureau, President's Secretariat, 2016). He highlighted not merely the graveness of the unease but also the need for counter actions.

As mentioned earlier Nation-States around the world are facing the most complex and intertwined menaces of global terrorism. In this scenario, State surveillance is tailored as a legitimate defence to protect democracy and freedom. At a conceptual level surveillance and democracy are antithetical and the relationship is complex, contextual and multifaceted. Its impact on our lives making it critical to understand the complexity of the relationship between each other.

Aftermath of Orlando Attack in United States (June 12, 2016), D.C. Pathak (former Director of IB) contended that preventive action taken on an intelligence assessment, if questioned in the human rights plane in all cases would weaken the security of a democratic state. He further argued that intelligence set up in a democracy is wedded to an apolitical pursuit of threats to national security and its professionalism would normally not be questioned by any other wing or agency of the government. (2016). Further, Uday Bhaskar (2005) argues that democracies remain vulnerable and if the freedom of personal movement is not to be ruthlessly curtailed, preventive measures will have to be reviewed and appropriate surveillance procedures introduced. In other words, it is often imperative for a functioning democracy to curtail the illegal behaviours and activities which can pose a threat to democratic intuitions (Haggery & Samatas, 2010, p.7). According to Kevin Haggerty and Minas Samatas (2010), democracy involves a system of open procedures for making decisions in which all members have an equal right to speak, have their opinions counted and for protecting individuals from the corrupting effects of power. Further, they assert that one of the significant things about democratic governance and surveillance is that the democracies are accountable to their citizens. The main contention being that democracy and surveillance can co-exist. It is due to that that despite opposition surveillance continues; it is believed that it is near impossible to penetrate complex criminal organisations through conventional police work.

In India, during post 9/11 and 26/11 scenarios, interception clauses were enabled through series of legislative reforms enacted after lackadaisical parliamentary debates. Even debates in civil society were eschewed in the name of national security or development of the state and were addressed with nationalist jingoism. Most appropriate case of eschewing would be Armed Forces (Special Powers) Acts implemented in particular areas which provided immunity and powers to armed forces to constantly monitor and surveil civilians from last five decades.

Such developments most importantly abridge the right to privacy and it gets more complex due to the sheer absence of persuasive jurisprudence of privacy protection supplemented with legislative silence in India. Contrary to the absence of privacy law, there are numerous laws which trample and trespass the right to privacy. In 2012,

the committee of experts on privacy, chaired by Justice A.P. Shah (Shah Committee) suggested among other things a constitutional basis for the right to privacy. The Committee highlighted how different forms of surveilling clauses have created an unclear regulatory regime which is non-transparent, prone to misuse and does not provide remedy for aggrieved individuals. The recommendations refer to the chequered history of telephone tapping and political snooping in the hands of the State and raise questions on the standard and procedural legal framework to safeguard individual privacy and personal liberty. Instead of looking at it narrowly as a privacy issue we must look into broader issues such what are the goals of State surveillance and the extent to which it is required to counter terror, protect national security and to streamline service delivery.

In this scenario, the major challenges for democracy and surveillance appears around constitutionalism and rule of law. Their basic idea is to maintain institutional restraints and insulate fundamental liberties from oppressive actions by the State by turning it into a subject of the law. Under the 'long decade' these notions were transformed, in response to changing threats to national security. To evade unpredictable catastrophic risks, uncertain and unanticipated threats, or any extra-ordinary and emergency situations, the Indian State created discretionary space to respond to these situations. Such discretionary space is what David Dyzenhaus calls as legal "black hole" and legal "grey hole", the former is "a situation in which there is no law," the latter is "a facade or form of the rule of law rather than any substantive protections" (Dyzenhaus, 2006, p.3).

The government instituted major intelligence organisations and surveillance infrastructure, without any legal basis or statutory existence, which is a legal "black hole." It gave enormous power to the executive without any accountability and transparency in their functioning. On February 23, 2016, Supreme Court dismissed Public Interest Litigation (PIL) from non-governmental organisation, Centre for Public Interest Litigation, to bring accountability and transparency in the functioning of intelligence agencies. The judiciary maintained that the intelligence agents are bound to have secrets which the courts could not scrutinise (Choudhary, 2016). Apart from this legislature, to address extra-ordinary situations and public emergency, it framed laws they are basically a legal "grey hole." It is not a lawless void, but a legal space in which there are some legal constraints on executive action. Even so the constraints are so insubstantial and inadequate that it is unlikely to provide substantive protections from potential dangers of unlawful surveillance and corrupt uses of power.

The dangers of surveillance do not merely arise from its use during emergencies; rather its use for ordinary purpose is far more lethal. The presence of political surveillance turned out as a dragnet to surveil and prevent oppositions, movements and disagreements against the Indian State and induce State's ideological and developmental discourse. In doing so, it limits the possibility of alternative political constituencies to emerge or become effective and it can have disastrous consequences for the prospect of nurturing a democratic public sphere (Haggery & Samatas, 2010, p.5). According to John Tropey (2000), the State monopolised the legitimate means of movement in modern century. Such monopolization gave immense power to the State to trace and

monitor individuals, then prevent and expropriate right to travel and right to freedom of expression. For instance in 2016 Gladson Dungdung's passport was impounded, in 2015 a look out circular was issued on Priya Pillai and prevented to travel abroad, and in 2014 Christian Mehta was deported. As Ashis Nandy (2010) has argued that with the development of modern technology, management systems and information control modern State's control over citizen's rights and freedoms are more absolute. Moreover, it leads to formation of a State which successfully plucks out the escape routes and maintains social order and management. In doing so surveillance by the State not only violates right to privacy and free movement but also inhibits freedom of expression.

The major challenge for democracy in India is to strike a balance between often-corrosive surveillance measures with civil liberties. The State has the power to monitor and control people. Even if there are laws, they are substantively fragile to protect the democratic rights and constitutional freedoms from unlawful surveillance and corrupt uses of power. In coming future the relationship between surveillance and democracy would remain unsettled until the issues such as constitutionalism and rule of law related to them are addressed.

References

Austin, L. M. (2015). Surveillance and the Rule of Law. Surveillance & Society, *13*(2), 295-299.

Bayly, C. A. (1996). *Empire and Information: Intelligence gathering and social communication in India, 1780-1870.* Cambridge: Cambridge University Press.

Bhaskar, C. U. (2005, July 11). London Attacks: Abiding Pattern of Global Terrorism. *Institute for Defence Studies and Analyses Comment.* Retrieved November 12, 2016, from http://www.idsa.in/idsastrategiccomments/LondonAttacksAbidingPatternofGlobalTerrorism_CUBhaskar_110705

Chawla, P. (1991, February 28). Scandalous revelations. *India Today.* Retrieved March 26, 2016, from http://indiatoday.intoday.in/story/secret-report-by-cbi-contains-shocking-details-of-phone-tapping-ordered-by-congressi-govts/1/317946.html

Choudhary, A. A. (2016, February 24). Some secrets must remain secret: SC on intel agencies. T*imes of India.* Retrieved March 12, 2016, from http://timesofindia.indiatimes.com/india/Some-secrets-must-remain-secret-SC-on-intel-agencies/articleshow/51115071.cms.

Cohn, B. S. (1996). *Colonialism and its Forms of Knowledge: The British in India.* Princeton, NJ: Princeton University Press.

Dyzenhaus, D. (2006). *The Constitution of Law: Legality in a Time of Emergency*. Cambridge: Cambridge University Press.

Fresh tapes on Gujarat government's surveillance emerge. (2013, December 15). *The Hindu.* Retrieved March 26, 2016, from http://www.thehindu.com/news/national/other-states/fresh-tapes-on-gujarat-governments-surveillance-emerge/article5460462.ece

Gitenstein, M. H. (2009). Nine Democracies and the Problems of Detentions, Surveillance and Interrogation. In B. Wittes (Ed.), *Legislating the War on Terror: An Agenda for Reform* (pp. 7-42). Washington, DC: Brookings Institution Press.

Government of India. Director General of Civil Aviation. (2014, October 7). Public Notice: Use of UAV/UAS for Civil Applications. Retrieved May 28, 2015, from http://dgca.nic.in/public_notice/PN_UAS.pdf

Government of India. Director General of Civil Aviation. (2016, April 21). Draft Guidelines for obtaining Unique Identification Number (UIN) & Operation of Civil Unmanned Aircraft System (UAS). Retrieved October 15, 2016, from http://www.dgca.nic.in/misc/draft%20circular/AT_Circular%20-%20Civil_UAS(Draft%20April%202016).pdf

Govt. to launch internet spy system 'Netra' soon. (2014, January 6), *Times of India.* Retrieved March 28, 2016, from http://timesofindia.indiatimes.com/tech/tech-news/Govt-to-launch-internet-spy-system-Netra-soon/articleshow/28456222.cms

Haggerty, K. D., & Ericson, R. V. (2000). The Surveillant Assemblage. *British Journal of Sociology, 51*(4), 605-622. doi: 10.1080/00071310020015280

Haggerty, K. D., & Samatas, M. (2010). Introduction: *Surveillance and democracy:* an unsettled relationship. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and Democracy* (pp. 1-16). New York, NY:Routlege-Cavendish.

India. Parliament. Rajya Sabha. (2014, July 7). Session 232, Unstarred Question No. 780. Centralised surveillance and interception system. Answer given by Kiren Rijiju, Minister of State in the Ministry of Home Affairs, Dated 16-07-2014 retrieved from http://mha1.nic.in/par2013/par2014-pdfs/rs-160714/780.pdf (India. Parliament. Rajya Sabha, 2014a).

India. Parliament. Rajya Sabha. (2014, July 7). Session 232, Unstarred Question No. 809. Centralised surveillance and interception system. Answer given by Kiren Rijiju, Minister of State in the Ministry of Home Affairs, Dated 16-07-2014 retrieved from http://mha1.nic.in/par2013/par2014-pdfs/rs-160714/809.pdf (India. Parliament. Rajya Sabha, 2014b).

India. Planning Commission, GoI. (2009, January 28). Notification. Retrieved March 22, 2016, from http://www.uidai.gov.in/images/notification_28_jan_2009.pdf

India. Press Information Bureau, President's Secretariat. President of India inaugurates Counter-Terrorism Conference-2016. (2016). Retrieved June 2, 2015, from http://pib.nic.in/newsite/PrintRelease.aspx?relid=136023

India. Second Administrative Reforms Commission. (2008). *Combatting Terrorism Protecting By Righteousness, Eighth Report.* Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/cgg/unpan045484.pdf

Jenkins, D. (2014). The Long Decade. In D. Jenkins, A. Jacobsen, & A. Henriksen (Eds.), *The Long Decade: How 9/11 Changed the Law* (pp. 3-27). Oxford: Oxford University Press.

Jenkins, D. (2016). Procedural fairness and judicial review of counter-terrorism measures. In M. Scheinin, H. Krunke, & M. Aksenova (Eds.), *Judges As Guardians of Constitutionalism and Human Rights* (pp.163-176). Cheltenham: Edward Elgar Publishing.

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

Lyon , D. (2008, September 28). *Surveillance Society.*Talk for Festival del Diritto, Piacenza, Italia. Retrieved March 22, 2016, from http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf

Lyon , D. (2009). *Identifying citizens: ID cards as surveillance.* Cambridge: Polity Press.

Nandy, A. (2010). The State. In W. Sachs (Ed.), *The Development Dictionary: A Guide to Knowledge As Power* (2nd ed., pp. 295-307). London: Zed Books.

Pathak, D. C. (2016, June 18). Orlando has lessons for the democratic world. Sunday Guardian. Retrieved November 11, 2016, from http://www.sundayguardianlive.com/opinion/5385-orlando-has-lessons-democratic-world

Posner, E., & Vermeule, A. (2007). Emergencies, Tradeoffs, and Deference. In *Terror in the Balance: Security, Liberty, and the Courts* (pp. 15-58). New York, NJ: Oxford University Press.

Posner, R. (2006). *Not a Suicide Pact: The Constitution in a Time of National Emergency.* New York, NY: Oxford University Press.

Scheinin, M. (2016). The judiciary in times of terrorism and surveillance: a global perspective. In M. Scheinin, H. Krunke, & M. Aksenova (Eds.), *Judges As Guardians of Constitutionalism and Human Rights* (pp. 177-200). Cheltenham: Edward Elgar Publishing.

Sharda, K.(2013, November 23). Leaked tapes: CBI says it has 5,851 recordings. DNA. Retrieved March 26, 2016, from http://www.dnaindia.com/india/report-leaked-tapes-cbi-says-it-has-5851-recordings-1470650

Singh, S. (2012, April 7). No secrets on Blackberry: Security services to intercept information after government gets its way on popular messenger service. Mail Online India. Retrieved May 26, 2015, from http://www.dailymail.co.uk/indiahome/indianews/article-2126277/No-secrets-Blackberry-Security-services-intercept-data-government-gets-way-messenger-service.html

Singh, S. (2013, June 22). Lethal surveillance versus privacy. *The Hindu.* Retrieved March 26, 2016, from http://www.thehindu.com/opinion/lead/lethal-surveillance-versus-privacy/article4837932.ece.

Singh, U. K. (2007). *The State, Democracy and Anti-Terror Laws in India.* New Delhi: Sage Publications.

Singh, U. K. (2012). Mapping anti-terror legal regimes in India. In V. Y. Ramraj, M. Hor, K. Roach, & G. Williams (Eds.), *Global anti-terrorism law and policy* (2nd ed., pp. 420-448). Cambridge: Cambridge University Press.

Singh, U. K. (2014). Surveillance Regimes in Contemporary India. In F. Davis, N. McGarrity, & G. Williams (Eds.), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (pp. 42-58). New York, NY: Routledge.

Singh, V. (2015, July 6). Government out to match Aadhaar, NPR data. *Indian Express. Retrieved March 28, 2016, from* http://indianexpress.com/article/india/india-others/government-out-to-match-aadhaar-npr-data/ (2015a)

Singh. V. (2015, July 24). Phone tapping row; MHA steps in. *The Hindu.* Retrieved March 26, 2016, from http://www.thehindu.com/news/national/phone-tapping-row-mha-steps-in/article7461295.ece (2015b)

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security.* New Haven, CT: Yale University Press.

Some secrets must remain secret: SC on intel agencies. (2016, February 24). *Times of India.* Retrieved March 28, 2016, from http://timesofindia.indiatimes.com/india/Some-secrets-must-remain-secret-SC-on-intel-agencies/articleshowprint/51115071.cms

Thiruvengadam, A.K. (2010). Asian judiciaries and emergency powers: reasons for optimism?. In V. V. Ramraj & A. K. Thiruvengadam (Eds.), *Emergency Powers in Asia: Exploring the Limits of Legality* (pp. 466-494). Cambridge: Cambridge University Press.

Torpey, J. (2000). *The Invention of the Passport: Surveillance, Citizenship, and the State.* Cambridge: Cambridge University Press.

Vermeule, A. (2014). Security and Liberty: Critiques of the Tradeoff Thesis. In D. Jenkins, A. Jacobsen, & A. Henriksen (Eds.), *The Long Decade: How 9/11 Changed the Law* (pp. 31-45). New York, NY: Oxford University Press.

Waldron, J. (2003). Security and Liberty: The Image of Balance. *The Journal of Political Philosophy, 11*(2), 191-210. doi: 10.1111/1467-9760.00174