# SURVEILLANCE, PRIVACY AND TECHNOLOGY: A COMPARATIVE CRITIQUE OF THE LAWS OF USA AND INDIA


## Abstract

This paper attempts to analyse the laws relating to the protection of privacy in two major jurisdictions of the world, *viz.*, the United States of America (US) and India. Despite vast differences in socio-economic and political realities, these two nations qualify as intriguing subjects for study. Their diverse demography, geopolitical structure and apparent independence from communitarian regulatory mechanisms seem to accord these nations a unique autonomy in creating an indigenous legal framework to cater to their culture-specific requirements. The paper analyses the disturbing trend that emerges from the similar placement of these nations with regards to the issue of privacy protection- one with the most robust, functional and detailed legislative framework and the other without any clear policy in place. The primacy given to national security over individual liberties seems to be an accepted phenomenon in both these jurisdictions.


## I Introduction

> There will come a time when it isn t They re spying on me through my phone anymore. Eventually, it will be My phone is spying on me .
>
> - Philip K. Dick[1]

THE RIGHT to privacy is generally accepted throughout the democratic world as a fundamental human right. Most nations today guarantee privacy as a right available to all its citizens, though in varying degrees. Thus, privacy effectively is a limited, but a fundamental right, universally granted. Privacy as a right has myriad facets. Essentially a privilege granted to individuals to protect their actions, choices and private opinions shared in the personal sphere from being exposed or scrutinised by the world at large, it is generally considered to be of paramount importance, especially in the modern globalised world. As a result, a clear mandate is reflected in the Constitution of most nations pledging to protect this virtue, wherein privacy of one s home and confidentiality of communication form the basic normative standards. This is evident from an overview of the formulations in the more modern

---

1 *Quotes about Surveillance, available at:* http://www.goodreads.com/quotes/tag/surveillance (last visited on Feb. 6, 2014).

2 Charles Fried, Privacy 77 *Yale Law.Journal* 475 (1967-68).

Constitutions,[2] which not only guard such rights more determinedly, they do so with a keen concern as to the specific requisites to enable such protection.

In contrast, some of the older Constitutions have often deciphered the essence of such a right within the existing framework of the law in place, and afforded similar protection to the same. Whereas, sometimes express provisions were absent, judicial construction has ensured that privacy found a place, equitable to the major fundamental rights and placed upon the state an equivalent onus of protecting it from arbitrary breach. The evolution of privacy as a foremost human right was furthered by the emergence of international human rights documents, adopted by a number of these nations as part of their legal system. Foremost amongst these are the International Covenant on Civil and Political Rights (ICCPR) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) . The Universal Declaration of Human Rights (UDHR)[3] and ECHR[4] amongst other international documents seek to protect arbitrary interference with one s private and family life. What is interesting to note, however, is the increased propensity with which alleged breach of this sacrosanct personal sphere is being committed in modern times, which necessitates a deeper introspection into the matter of its protection.

The peculiar nature of this right can perhaps be best understood by attempting to understand, first, the meaning of privacy . As soon as Warren and Brandeis seminal work[5] on the right to privacy was published, one encountered the first acceptable definition of privacy as the right to be left alone . This definition, although criticised later to be broad and dated, continues to serve as a useful reminder of the essential nature of the right, despite the simplicity and generality of its construct. Modern definitions of privacy generally include the following categories of rights, all of which form separate but indispensable components of the right to be left alone :[6]

---

3 The Universal Declaration of Human Rights, art. 12 reads:

> 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.

4 European Convention on Human Rights, art. 8.

5 Samuel Warren and Louis Brandeis, The Right to Privacy 4 *Harvard Law Rev.* 193 (1890), *available at:* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (last visited on Sep. 8, 2015).

6 Micheal Friedewald, *et al.*, Seven types of privacy (2013), *available at*: http://works.bepress.com/cgi/viewcontent.cgi?article=1070&context=michael_friedewald (last visited on Oct. 8, 2015).

i. Privacy of the home, or domestic privacy- dealing with activities within the territorial limits of the home, the place of work and including public places;

ii. Privacy of information, or data privacy- dealing with the regulatory framework relating to the managing of personal information (data preservation and dissemination);

iii. Privacy of the body, or physical privacy- dealing with the freedom from invasion of the physical self; and

iv. Privacy of communication- dealing with the protection of communication via any known legal medium.

There is until now, however, no universally accepted definition of privacy. Despite this, the importance of protecting privacy against arbitrary breach is generally considered so paramount that though its definition is disputed, its protection is undisputed, which perhaps serves as the greatest inspiration behind the current study.

The gigantic advancement in technology and its contribution in the spread of surveillance by state actors has been at the root of much debate in the judiciary and academia alike. The possibility of gathering an individual s privileged information by both state and non-state players employing sophisticated technology is more fact than fiction. Most legal systems fail to wholesomely account for the modernisation in technological infringement techniques in their protective measures. Municipal laws, by and large, have relied upon developing directives and model codes of conduct in data collection, especially with regards to mass surveillance exercises; ironically, taking advantage of the void they choose to maintain. The proliferation of anti-terrorist legislations perhaps create the greatest anomaly, within which the state is empowered to infringe upon individual space in an unforeseen manner, with as little regulation and accountability as may be afforded under the aegis of democratic framework. The unstated acceptance by nations of the necessities of gathering intel and the consequential involvement of issues concerning the safety and security of the state, possibly is the single largest threat to the anonymity and desire for secrecy of the citizen; and as shall be discussed in the course of this paper, this is generally found to be the compelling reason by courts to allow such intrusion in the interest of national security .

This paper attempts to analyse the laws relating to the protection of privacy in two major jurisdictions of the world, *viz.*, the US and India. Despite

vast differences in the socio economic and political realities, these two nations qualify as intriguing subjects due to these very same distinctions. Their diverse demography, geopolitical structure and apparent independence from communitarian regulatory mechanisms (as distinct from their European counterparts, for example) seem to accord these nations with a unique autonomy in creating an indigenous legal framework to cater to their culture-specific requirements. Further, the unnatural abundance of laws within the US system that deal with surveillance and privacy, especially in the post-9/11 scenario, and the complete absence of the same in India and the justifiable need to create its own distinct framework, makes for an exceptional analysis.

Initiating the debate on privacy protection in the US, the Brandeis article led the US courts taking up the cause with serious concern. The US is a signatory to the ICCPR, and since the US legal framework includes all international obligations as binding upon its citizens, this makes *inter alia* the right to privacy a fundamental right under its laws. Further, through the emphatic pronouncements by the US Supreme Court in several cases before it, and most specifically in *Griswold* v. *Connecticut* [7] the right to privacy was accorded constitutional status in no uncertain terms. Inspite of the judicial resolve, with possible origins in the cold war era, state-sponsored surveillance has been a known feature of the US foreign policy.[8] Activities relating to gathering of intelligence about Soviet Unions actions however, soon displayed an alarming propensity for illegal intrusions into the lives of the common citizens. Despite severe criticisms, this trend continued till the disintegration of Union of Soviet Republics (USSR) in the early 90s, and revived again post-9/11 at an unprecedented scale. At present, the US has the greatest number of laws relating to surveillance, search and seizure far greater than all the other major powers in the world.

In India, the constitutional status of privacy as a right was first espoused in the dissenting opinion by Subba Rao J in *Kharak Singh*,[9] who was in favour of expanding the interpretation of the right to life and personal liberty granted under article 21 of the Constitution to include a tacit right to privacy. However, it was finally in *Govind* v. *State of Madhya Pradesh*[10] that the apex

---

7 381 U.S. 479 (1965).

8 Peter P. Swire, The System of Foreign Intelligence Surveillance Law 72 *Geo. Wash. Law Rev.* 1306 (2003-04).

9 *Kharak Singh* v. *State of U.P.* (1964) 1 SCR 332.

10 *Govind* v. *State of Madhya Pradesh* (1975) 2 SCC 148.

court accepted the right as part of the right to personal liberty, *albeit* within a limited sphere of operation. This was furthered by the court's observation in *Rajagopal:*[11]

> the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a right to be let alone. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters.

This dictum has thereafter been followed quite consistently in *PUCL* v. *Union of India*,[12] and *State of Maharashtra* v. *Madhukar Narayan Mardikar*,[13] though the legislature has shown little interest in creating the necessary framework for protection of these rights, other than the controversial draft privacy bill, leaked on the internet, which is yet to be tabled in the Parliament.

Despite such clarity of intent, however, it is incumbent upon governments that greater safeguards be afforded for protection of individual privacy, as major perpetrators of breach in this case are governments themselves. In the interest of national security, governments breach individual privacy owing to the lack of effective machinery in order to protect the same. Thus, the real question is, can the government protect the citizens from itself? The answer to this alone can guarantee the desired consequences for our common future.

**Identifying the subjects: US and India**

The reason for identifying the US legal system as a frame of reference, wherein the Indian position can be contrasted, is primarily twofold. *First*, it is one of the oldest legal systems of the world where privacy as a basic right found its acceptance; privacy was firmly embedded in the American constitutional discourse as a right in itself. This is quite unlike in the United Kingdom (UK) where as late as even the late 20th and early 21st century, courts were grappling with the idea of incorporating privacy into the law of torts, under breach of confidence or malicious falsehood.[14] This is the reason

---

11 *R.Rajagopal alias R.R.Gopal* v. *State of Tamil Nadu* (1994) 6 SCC 632.

12 1995 SCC, Supl. (2) 572; JT 1995 (3) 365.

13 AIR 1991 SC 207.

14 The English law on privacy has more modern foundations. Despite Cooley's J pronouncement that privacy amounted to the right to be let alone, there was no separate law of privacy in the UK, as found by LJ Glidewell in *Kay* v. *Robertson* (1991) FSR 62.

why a comparison with the American legal model would be, in the opinion of the author, more appropriate.

The *second* reason for choosing the US would be that, much like India, America has also been forced to undergo sweeping legal changes with respect to issues of privacy and surveillance post a landmark terror attack, namely the 9/11 attacks.[15] Therefore, national security came in as the overarching justification making use of which a lot of critical constitutional concerns such as privacy and individual liberty were brushed aside and *prima facie* draconian laws like the PATRIOT Act[16] and the concomitant use of surveillance and interception were validated. Further, the PATRIOT Act is not restricted in its application to merely countering terrorism, but is bestowed with wider powers in ordinary criminal and investigative matters. In India also, while the cabinet discusses several modifications to the imminent Privacy Bill, and attempts to garner public opinion in order to authenticate the same, the lurking fear of a threat to national security continues to be a recurring theme in any such campaign. These factors, coupled with a similarly diverse demographic and peculiar geopolitical structure, set up the justification behind the said equivalence being drawn.

## II Evolution of the American jurisprudence on privacy and surveillance: A brief overview

In the US, the need for a law to protect privacy was articulated as early as 1890, when Warren and Brandeis published an article titled The Right to Privacy .[17] This article laid the intellectual foundations for the law on privacy.[18]

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right to be left alone . Instantaneous photographs and newspaper

---

15 This position finds concurrence in India, where post the 26/11 terrorist attacks in Mumbai, national security measures were sought to be introduced at an unprecedented scale. This, normatively, included greater autonomy granted to investigative agencies in collection of intelligence, as evident from the draft bill on the right to privacy. See generally, full text of the bill with attorney general s comments, *available at*: http://cis-india.org/internet-governance/draft-bill-on-right-to-privacy (last visited on Sep. 8, 2015).

16 *Available at*: http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (last visited on Oct. 15, 2015).

17 Samuel Warren and Louis Brandeis, The Right to Privacy 4 *Harvard Law Rev.* 193 (1890).

18 *Ibid.*

> enterprise have invaded the sacred precincts of the home private devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house tops ... The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery... The intensity and complexity of life attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by bodily injury. It is our purpose to consider whether the existing law affords a principle which can be properly be invoked to protect the privacy of individual; and, if it does, what the nature and extent of such protection is...

The American courts trace the origins of the right to privacy as being associated with the right to property. But gradually the courts recognised that the protection of privacy must transcend property rights. In *Warden* v. *Heyden*,[19] the US Supreme Court declared:[20]

> The premise that property interests control the right of the Government to search and seizure has been discredited.... We have recognized that the principal object of the fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.

The most well known American cases on privacy are *Griswold* v. *Connecticut*[21] and *Roe* v. *Wade*.[22] *Griswold* concerned a constitutional challenge to a law which prohibited the use of contraceptives. Upholding the notion of privacy, Douglas J of the US Supreme Court held:[23]

---

19 387 US 294.

20 *Ibid*.

21 *Supra* note 7.

22 410 US 113 (1973).

23 *Supra* note 7.

> Governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.... Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.

Striking down the concerned legislation as an unconstitutional invasion of the right to marital privacy, it was held that the right of freedom of speech and the press includes not only the right to utter or to print but also to distribute, receive and read and that without those peripheral rights, the specific right would be endangered.

*Roe* v. *Wade*[24]concerned the right of an unmarried pregnant woman to an abortion. Upholding the woman s right to make that choice which concerned her private life, the US Supreme Court held that although the US Constitution did not explicitly mention any right of privacy, the US Supreme Court itself recognised such a right as a guarantee of certain zones or areas of privacy and that the roots of that right may be found in the first amendment, in the fourth and fifth amendment, in the penumbras of the Bill of Rights and in the concept of liberty guaranteed by the fourteenth amendment. [25]

Surprisingly little legislation was found to operate within the US that dealt directly with the issue of privacy, till before the world trade centre tragedy in 2011, at the national level. Post the Watergate fiasco and the era of J. Edgar Hoover, however, a single legislation in this field surfaced, which attempted to restrict governmental disclosure of private information, irrespective of the purpose of such collection. This statute was the Privacy Act of 1974.[26] This document had a number of useful provisions, including the use of private individual records for no other purpose but the documented utility which may be used by executive agencies upon furnishing a request in writing for the same. It includes the anonymity clause- in utilising packet

---

24 *Supra* note 22.

25 Detailed discussion on the judicial protection of privacy in the US can be found in Richard Posner, The Uncertain Protection of Privacy by the Supreme Court 1979 *Sup. Ct. Rev.* 173 (1979).

26 Michael Walter-Echols, Panopticon Surveillance and Privacy in the Internet Age (2009), *available at:* https://www.wpi.edu/Pubs/E-project/Available/E-project-022709-132355/unrestricted/Panopticon.pdf (last visited on Sep. 15, 2015).

data, or in statistical analyses, personal identity could not be disclosed, which was an extremely progressive measure adopted by the Congress, considering the period in which this law was enacted.[27] The consent approach has also been adopted in cases concerning the transfer of this data to other authorities, including government agencies, which again is a salient feature of this statute, violations under which were punishable by imprisonment and fine, or both a bold step in the age of government surveillance, generally.

The Health Insurance Portability and Accountability Act, 1996,[28] is the only other legislation, which deals with essential privacy concerns, though its focus is entirely on the healthcare sector. The primary protection afforded by this legislation pertains to the non-disclosure of information regarding any person who avails of healthcare and insurance services relating to the same, without express authorisation being granted by such individual. However, there is enlisted a set of exceptions where disclosure is permitted, in the interest of the patient, the insurance company and in certain circumstances, law enforcement. There are similar penalties for violation as in the case of the previous Act, and the disclosure should adhere to the minimum requisite level in order to fulfill the purpose for the same.

With the introduction of more stringent security measures during the Bush administration, however, exceptions were carved out in the Privacy Act, 1974 to accommodate the newly adopted policy. The exemption granted to homeland security enables it to track passengers based on the information in their boarding passes and other mandatory disclosures made to the airliners and airport authorities. This situation can be extremely tricky, owing to the diverse nationalities of passenger traffic through the US. The conflict of laws is solved through the grant of this immunity to investigative agencies; however, the question remains regarding the extra-territorial application of such laws, wherein the foreign nationals are subjected to the scrutiny of the Home Department of the US with no law to protect their privacy, since their native law is inapplicable in the US and they fall entirely outside the purview of domestic US laws and their protection.[29]

---

27 *Ibid.* This is perhaps the first known legislative utilisation of the anonymisation of data, a regular feature in modern data protection regimes.

28 Public Law 104-191, *available at*: https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/hipaalaw.pdf (last visited on Oct. 10, 2015).

29 Casper Bowden, The U.S. Surveillance Programmes and Their Impact on E.U Citizen s Fundamental Rights (2013), *available at:* http://www.europarl.europa.eu/meetdocs/

Despite the presence of a mechanism for the protection of privacy, however inadequate, the US has had a history of acts violating individual privacy since the cold war era. Wiretapping and bugging were commonly used political tools, employed by governments to preempt opposition politics, corporate espionage, *etc.* The origin of such acts can be traced back to the cold war period, when the US, the USSR and their respective allies engaged in every conceivable means for gathering intelligence about the ongoing activities and strategies of the adversary. This process often entailed covert surveillance of subjects, including both American and non-American citizens, some of whom were beyond the domestic jurisdiction of the US.[30] Although there existed the impending dangers associated with a world war for a third time, of far greater magnitude than what the world had witnessed, with the possibility of devastating consequences, little justification can be provided for a number of grave human rights violations such an environment brought in its wake.[31]

The advancement in technology and proliferation of especially the electronic media has brought to light a number of such violations committed on the part of the state, which under any civilized framework would be difficult to justify. Years later, when Federal Bureau of Investigation (FBI) classified files were brought into the public domain, did the world gain knowledge of their continuous surveillance of civil rights champion Martin Luther King, Jr., a practice that continued unto his death. The US National Security Agency (NSA) backed project ECHELON,[32] which was the first worldwide revelation of the extra-terrestrial application of surveillance by the US, came under heavy criticism for not only targeting enemy states but also neutrals and allies. The European Parliament, concerned about the adverse impact this programme had on their domestic affairs and foreign relations, issued a directive to all member states to use encryption in communication

---

2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf (last visited on Oct. 8, 2015).

30 Anders Lagerwall, Privacy and Secret Surveillance from a European Convention Perspective (2008), *available at:* http://www.adbj.se/2009/ht_2009_Anders_Lagerwall.pdf (last visited on Oct. 8, 2015).

31 William M. Beaney, The Right to Privacy and American Law 31 *Law & Contemp. Probs.* 253 (1966).

32 *Supra* note 29; generally contains scathing criticism of the extra-territorial application of ECHELON, as well as other US Government surveillance projects and their impact on EU nations.

to avoid sensitive information leakages. Interestingly, the ECHELON and related programmes were continued till recently by the US.[33]

The Nixon years and the Watergate controversy[34] marked the beginning of a new era of data protection and anti-surveillance movements within the country. Following the resignation of President Nixon, the Senate-appointed committee which investigated the mass surveillance and politically motivated targeting of opposition members, found that such measures were adopted under the authority of the White House itself, and in cases involved the accidental collection of data pertaining to trans-border communication. Despite condemning the ongoing mass intrusion into the lives of unsuspecting citizens, they concluded that such lapses were an occupational hazard of intelligence collection unfortunate but necessary nonetheless. They focused their efforts, instead, on trying to reduce the damage, rather than correcting it, and this approach found its way into American public policy through the introduction of Foreign Intelligence Surveillance Act in 1978, which regulated the surveillance activities to be carried on by governmental agencies, as well as other actors, since. The interception of information relating to non-Americans, however, remains unresolved, and international law is significantly silent on this issue.

The aftermath of the 9/11 attacks prompted the US Congress to pass, within six weeks of the disaster, the PATRIOT Act, which provided for unforeseen autonomy to investigative agencies to employ surveillance initiatives to counter terrorism, while simultaneously reducing judicial supervision and accountability for the same. The PATRIOT Act, along with NSAs controversial warrantless surveillance program were instruments used by the state to carry out mass surveillance activities on millions across the world, in its efforts to gather intelligence during its much hyped war against terror . Other measures included the likes of Operation TIPS (Terrorism Information and Prevention System) and homeland security, both of which supplemented the pre-existing framework of surveillance.[35]

---

33 *Ibid*.

34 Nixon the 37th President of the United States, serving from 1969 to 1974. The Watergate scandal escalated in 1973 costing Nixon much of his political support and on Aug. 9, 1974, he resigned from office.

35 Ann Cavoukian, *National Security in a post-9/11 world: Rise of Surveillance... The Demise of Privacy*? (2003), *available at*: https://www.ipc.on.ca/images/resources/up-nat-sec.pdf (last visited Nov. 10, 2015). A brief analysis of US Surveillance programmes undertaken by the authors reveals the impact of these measures on

Operation TIPS, was especially problematic owing to it involving workers, with access to the interiors of people s homes, to be recruited as volunteers in the unique position of being able to perceive threats or potential terrorist activities from close quarters. Passed under the Homeland Security Act, 2001, this campaign came under heavy criticism and was finally removed. Under the Department of Homeland Security,[36] the consolidation of several departments of the government, barring the FBI and CIA, took place, with the purpose of streamlining and systematising their working. The department had a major function of accessing, receiving and analysing information collected *via* intelligence agencies amongst others, but including law enforcement agencies, private sector entities and the like for the purpose of identifying and assessing potential terrorist activities. The array of such measures included others like the terrorist information awareness, a research initiative enabling active preemption of terrorist threats through identification, processing of information and ultimate action in preventing the US from likely attacks in the future. This information included transactional details available from any purchase or exchange made by the suspects. In conjunction with this was the passenger information system, which profiles international passengers who avail transportation within or through the US, and in cases involving suspected individuals, security measures are initiated to neutralize any threat they might pose. These initiatives, backed heavily by the national security rhetoric, ushered in the new era of surveillance in the American system, with the PATRIOT Act, as their frontrunner.

**The PATRIOT Act, 2001**

In the aftermath of the 9/11 attacks, the US Congress passed hastily the legislation which was to become the touchstone for all future American action against terrorism. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001, better known as the PATRIOT Act,[37] is the single most controversial piece of

---

citizens, and the response to the same by the judiciary, who have largely been conformist in attitude with regards to issues of national security. The primacy accorded to national security concerns seems to be a regular feature in post-9/11 judicial decisions.

36 America s Surveillance Society, *available at:* https://www.aclu.org/files/images/asset_upload_file381_37802.pdf (last visited on Nov. 8, 2015).

37 Jennifer Chandler, Privacy versus National Security- Clarifying the Trade-off , *available at*: http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_07.pdf (last visited on Oct. 8, 2015).

legislation passed in the US since the Reagan era, and continues to operate amidst much debate about the unbridled surveillance powers handed over to the investigative agencies under the pretext of prevention of terrorist activities aimed against the country.

In order to understand the origins of the Act, one has to appreciate the socio-political climate of the nation at the time of its passage.[38] The atmosphere of insecurity amongst the populace and the helplessness of the law enforcement agencies, prompted a charged Congress into debating whether the intelligence agencies required greater autonomy in their functioning in order for it to tackle future threats, which it was incapable of doing within the existing framework of the excessively stringent civil liberties law.[39] In its zest to act on the occasion, the legislature, aided by the persuasion of the neoconservatives who were strongly represented in the Bush cabinet, enacted this law which made numerous changes to the surveillance mechanisms, judicial procedure and immigration laws.

Despite the criticism faced by the successive Bush governments as a result of the measures adopted under the Act, which a number of its detractors claimed led to a *per se* violation of the First Amendment to the US Constitution (most of whom were democrats, ironically), some of its more controversial provisions, including the provisions related to roving wiretaps and surveillance targeting lone wolves upon mere suspicion, were extended twice during the tenure of Barack Obama on account of the PATRIOT Sunsets Extension Act of 2011.[40]

The major discomfort surrounding the PATRIOT Act emanated from a plethora of provisions, which inarguably strike at the very heart of basic civil liberties. At the epicenter of this controversy are two titles from the Act, namely, title II and title V.

Ominously named enhanced surveillance procedures , title II deals with government agencies carrying on surveillance activities with respect to any suspected terrorist action or potential threat source. This interestingly, includes a wider ambit which becomes apparent at first sight. The possibility of gathering foreign intelligence, an accepted roadblock in case of criminal investigation

---

38 *Ibid.*

39 Beryl A. Howell, Seven Weeks: The Making of the USA PATRIOT Act 72 *Geo. Wash. L. Rev.* 1145 (2003-04). ,

40 *Ibid.*

in the past was removed by making necessary amendments to the FISA. Information sharing procedures were simplified and the previous requirement for proving a non-citizen to be part of foreign espionage was removed, for aid of surveillance process.

The increase in the ambit of surveillance measures undertaken, under this part, which included surveillance being carried out on packet networks; and the ability to route and address was provided within this, leaving the scope for collecting innocent data. It further empowered district courts to order for surveillance measures in cases concerning possibility of terrorist involvement. The process for demanding the disclosure of private electronically stored information was made lenient, insofar as the wavering of stringent procedural safeguards of the wiretapping laws are made, which allow access to protected computers including those outside the domestic jurisdiction of the US. Voluntary sharing of customer information by internet service providers was mandated of any kind of suspicious activity on their network, under the apprehension of imminent danger.

Sneak and peek warrants, issued by the Federal Bureau of Investigation (FBI) to subjects, permitted a delayed notification, wherein delay was left undefined in the aid of the investigative agency for the purpose of ensuring an amount of flexibility. The court however, disallowed this practice as violative of the fourth amendment to the US Constitution.[41]

The other area of unease regarding this section relates to the use of the roving wiretap technique.[42] The ability of terrorists to evade traditional wiretap techniques, which are by themselves more difficult to procure, renders conventional methods redundant. This provision enables a single order by a competent court, granted with lesser disclosure or specifications, to be used for continual tracking of individuals, irrespective of the change in location or devices used by them. Along with this comes the hotly debated regulation empowering the FBI in any inquiry pertaining to suspected terrorist activities, to ask for the documents or records, digital or otherwise, from any authority within the US.[43] This created a great furor amongst various sections of society,

---

41 Andrew E. Taslitz, The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions 65 *Law & Contemp. Probs.* 125 (2002).

42 Neil M. Richards, The Dangers of Surveillance , *available at:* http://harvard lawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf (last visited on Nov. 8, 2015).

43 Nick Taylor, State Surveillance and the Right to Privacy , *available at:* http:// www.surveillance-and-society.org/articles1/statesurv (last visited on Sep. 18, 2015).

especially institutions, who were unwilling to give up the records maintained by them for fear that their clientele be targeted upon mere suspicion. However, no specific instance of record seeking or subsequent denial of the same has come to light till date.

Certain controversial elements under the title were set to expire, including roving wiretap, foreign intelligence gathering, and the authority to intercept communication, record seeking and a number of related provisions. However, upon the extension being granted, these continue to be in force as of this day.

In addition to title I, which primarily revolves around means to augment the efficacy of the war on terror and protection of internal security, title V of the Act attempts to remove roadblocks from the path of the investigative agencies, especially when dealing with cases pertaining to international terrorism. Titled removing obstacles to investigating terrorism , this chapter seeks to induce cooperative participation of citizens in fighting terrorism.[44] The incentivisation of dissemination of information with regard to terrorist activities, or for the assistance in the demolition of terrorist outfits, was ensured through financial benefits. Federal agents were allowed to share information with the central body, in the hope that this shall enable greater access for both in cases of conflicting jurisdictions. The investigative ambit of the secret service was increased, and the wider powers included the domain of electronic device related offences, and production and maintenance of records made simpler and validated by the effect of this section.[45]

However, the most problematic area under this title was the issue of national security letters (NSLs),[46] which are essentially executive dictums demanding the submission of all material records of the recipient, pertaining to the subject matter of the enquiry along with an order requiring the said body to keep such communication confidential. This effectively took away the rights of the subjects from disclosing that they were under surveillance, and to seek judicial intervention. Such NSLs could be issued by the FBI, allegedly by the Central Intelligence Agency (CIA) and other governmental bodies, and did not require the authorization of the director or any high-

---

44 Daniel J. Solove, Reconstructing Electronic Surveillance Law 72 *Geo. Wash. L. Rev.* 1264 (2003-04).

45 Christopher Slobogin, The Meaning of Intellectual Privacy 87 *Tex. L. Rev.* 25 (2009).

46 *Ibid.*

ranking officer. Agents of these bodies in charge of the investigation were found qualified for this purpose.[47] When the constitutionality of these gag orders were challenged in court, on the grounds that they breached the right to constitutional remedies and privileged communication between client and advocate, the court upheld the same and the gag order requirement was consequently relaxed.

**Controversies surrounding the PATRIOT Act**

The PATRIOT Act, one of the more voluminous publications of the US Congress, has been criticised on various grounds, of which one pertains to the haste with which this bill was moved through the two houses before adoption. Senators and congressmen have severally complained of their inability to undergo a closer scrutiny of its contents, due to the paucity of time.[48] While this is partially due to the charged political atmosphere which demanded action from the legislature, skeptics suggest that the bill was framed prior to the attacks, and the tragedy of 9/11 merely created the perfect opportunity for the government to push it through. If a parliamentary committee was set up, and the bill in its entirety inspected more precise, perhaps greater safeguards for civil liberties and balancing the concerns for security could be achieved irrespective of the immediate needs.

In order to remedy the growing discontent with the workings of the Act, certain changes were introduced to the original legislation.[49] This was done with a view to help increase its acceptability amongst its detractors, especially those who were not against the Act *per se*, but demanded a more reasonable approach be reflected in it. The most important changes were with regards to increased congressional oversight, which lent a flavor of accountability to the legislation, by making the investigative authority ultimately responsible to the Congress. The acceptance of the requirement for providing a reasonable notice to subjects under the Act was another major breakthrough, as was the moderation of wiretap provisions, orders for which can not be so easily obtained presently. Making authorities answerable for their ultimate acts and omissions is undoubtedly a progressive step by the legislature in this regard.

The issues regarding the roving wiretaps provision is largely related to the surveillance of a person upon mere suspicion, and the complete absence of hard evidence. Most scholars agree that this would be a classic case of the

47 *Ibid.*
48 *Supra* note 39.
49 *Ibid.*

Big Brother syndrome, wherein a person is under constant surveillance of the state, and includes a significant possibility of failure to incriminate. Thus, the recorded infringement of a person s privacy can thereafter be used against him for a variety of purposes. Further, the probability of other related persons being under state observation plainly due to shared usage of an electronic communication device is a threat unrecognized under these blanket measures.[50]

Wiretapping and other surveillance technologies having improved, it is but natural for states to desire their usage for the purpose of self-preservation. However, the advancement in technology ought to entail an additional responsibility.[51] In case of the PATRIOT Act, the complete removal of any requirement for accessing or handling data responsible creates an atmosphere of suspicion, as in the case of a police state. The access to voicemails without an authoritative order, merely based on a common warrant issuable by trial courts made possible under the statute; the NSLs, which flout the basic civil rights, are championed by the state as necessary tools, whereas the powers of arbitrary search and seizure, as effectively legalised under this scheme, are deemed unconstitutional in even the less developed democracies. The same is true in the case of record-seeking provisions, which form a framework of subterranean surveillance, by identifying patterns of behavior of sections of the populace in order to find criminality of intent . The other important aspect is the extra-territorial application of these surveillance techniques, which in effect, has the potential of carrying out such activities targeted at foreign nationals, with scant regard to their right to privacy, or the data protection regime prevalent in their home state or habitual residence.[52]

Representative Jim Sensenbrenner, the Republican congressman from Wisconsin, responsible for introducing the first draft of the PATRIOT Act, at the floor of the house in 2001 stated:[53]

---

50 Adam D. Moore, Privacy, Security and Government Surveillance: Wikileaks and the New Accountability (2011), *available at*: https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofsecrecy/papers/reading/Moore.pdf (last visited on Aug. 8, 2015).

51 United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue, 2013), *available at*: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (last visited on Sep. 8, 2015).

52 *Ibid*.

53 *Available at* http://www.brainyquote.com/quotes/authors/j/jim_sensenbrenner.html (last visited on Aug. 8, 2015).

> While I believe the Patriot Act appropriately balanced national security concerns and civil rights, I have always worried about potential abuses. Seizing phone records of millions of innocent people is excessive and un-American.

In a recent report by the President s review group on intelligence and communications technologies, similar concerns were raised.[54] Through the 300 page long document, the group strongly recommended that effective action be taken for development of technology wherein individual rights are not unnecessarily tampered with; regular disclosure by the government and subjects of surveillance; careful determination of the purpose behind each surveillance measure adopted and highlighted the understated need for protection of the most basic of all human freedoms, the right to be let alone.

## III Indian position: A judicial construct

The right to privacy in India has originated from two distinct sources: the law of torts and constitutional law. The tortuous liability arising out of breach of the private space by unlawful means, which has been recognised by law courts across the world as a means of protecting privacy finds its place within the Indian framework, though in a limited manner. Invasion into the privacy of a person under tort law, especially relating to individual s family and matrimonial matters, procreation, education and the like, are actionable as such, except in situations where either the publication of such information falls within the public domain, or is done by a public servant in the course of his employment, for a lawful purpose unless the publication of such information is proved to be false or malicious.[55]

Privacy rights in the Indian context are primarily a judicial construct. The right to privacy is not expressly dealt with in the Constitution, either as a separate right or an exception to freedom of speech and expression under article 19(2), enumerating the various reasonable restrictions that are imposed upon them. This however, has not deterred courts from creating a framework for privacy protection within the constitutional scheme. They read into the meaning of article 21, the fundamental right to life and personal liberty, and

---

54 President s Review Group on Intelligence and Communications Technologies, Report on Liberty and Security in a Changing World (2013), *available at*: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last visited on Sep. 8, 2015).

55 M.P. Jain, *Indian Constitutional Law* (Kamal Law House, Calcutta, 2003).

found privacy to be implied therein, though in a limited sense. This interpretation has allowed privacy to be protected as a constitutionally guaranteed fundamental right, while limiting its scope by harmonious construction *vis- -vis* the freedom of the press under article 19 (1) (a).[56]

The first few cases that presented the Indian Supreme Court with the opportunity to develop the law on privacy were cases of police surveillance. The court examined the constitutional validity of legislations that empowered the police to keep a secret watch on the movements of an individual. The first of these cases, *Kharak Singh s* case[57]challenged the constitutional validity of regulation 236 of the Uttar Pradesh Police Regulations, 1861 which permitted surveillance. A majority on the bench struck down regulation 236(b) that authorized domiciliary visits as being unconstitutional but upheld the other provisions under that regulation. The majority was unreceptive to the idea of recognizing a right to privacy and dismissed the claim on the ground that there could be no fundamental right to protect mere personal sensitiveness . Their view was based on the conclusion that the infringement of a fundamental right must be both direct as well as tangible and that the freedom guaranteed under article 19(1) (d) was not infringed by a watch being kept over the movements of a suspect.

It was, however, the minority view expressed by Subba Rao J that laid the foundations for the development of the law in India. Subba Rao J held that the concept of liberty in article 21 was comprehensive enough to include privacy and that a person s house, where he lives with his family is his castle and that nothing is more deleterious to a man s physical happiness and health than a calculated interference with his privacy. The conclusion was that surveillance by domiciliary visits and other acts under regulation 236 was *ultra vires* articles 19 (1) (d) and 21.

In *Govind* v. *State of M.P.*,[58] also a case of surveillance under the Madhya Pradesh Police Regulations, the Supreme Court acknowledged a limited right to privacy. Yet, the court upheld the impugned regulation which authorised domiciliary visits in its entirety. This was on the ground that the object of the provision was the prevention of crime. The court held:[59]

---

56 *Ibid.*
57 *Supra* note 9.
58 *Supra* note 10.
59 *Ibid.*

> Depending on the character and antecedents of the person subjected to surveillance as also the object and the limitation under which surveillance is made, it cannot be said surveillance by domiciliary visits would always be unreasonable restriction upon the right of privacy. Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right that fundamental right must be subject to restriction on the basis of compelling public interest. As regulation 856 has the force of law it cannot be said that the fundamental right of the petitioner under Article 21 has been violated by the provisions contained in it: for, what is guaranteed under that Article is that no person shall be deprived of his life or personal liberty except by the procedure established by law .

*R. Rajagopal* case[60] is a watershed in the development of the Indian law of privacy. For the first time, the Supreme Court discussed the right to privacy in the context of the freedom of the press. The case concerned the right of the publisher of a magazine to publish the autobiography of the condemned prisoner, Autoshankar . The respondents contended that the intended publication (which was to expose some sensational links between the police authorities and the criminal) was likely to be defamatory and therefore required to be restrained. The issue of the right to privacy came up in this context. The Supreme Court held that the press had the right to publish what they claimed was the autobiography of Autoshankar in so far as it appeared from the public records, even without his consent or authorization. However, if the publication went beyond the public record and published his life story that would amount to an invasion of his right to privacy. Similarly, the government and prison officials who sought to protect themselves (by ostensibly seeking to protect the privacy of the incarcerated prisoner), did not have the right to impose a prior restraint on the publication of the autobiography; their remedy, if at all, could arise only after the publication.

The court recognised two aspects of the right to privacy: (i) the tortuous law of privacy which affords an action for damages resulting from an unlawful invasion of privacy and (ii) the constitutional right to be let alone implicit in the right to life and liberty under article 21. A citizen has the right to safeguard his own privacy, that of his family, marriage, procreation parenthood, child

---

60 *Supra* note 11.

bearing, education *etc.* and no person has the right to publish anything relating to such matters without the consent of the person concerned. The court acknowledged two exceptions to this rule: *first*, where the matter has become a matter of public record, the right to privacy no longer subsists. *Second*, public officials are not entitled to claim privacy when the act or conduct in question relates to the discharge of their official duties. Even where the publication is based upon facts found to be untrue, the public official is not entitled to protection unless it is shown that the publication was made with reckless disregard for truth. It is sufficient for the publisher to show that he acted after a reasonable verification of facts.

*People s Union for Civil Liberties* v. *Union of India* [61] was a challenge to section 5(2) of the Telegraph Act, 1885 which permits the interception of messages in cases of public emergency or in the interest of public safety. The Supreme Court held that the right to privacy included the right to hold a telephone conversation in the privacy of one s home or office and that telephone tapping, a form of technological eavesdropping infringed the right to privacy. The court found that the government had failed to lay down a proper procedure under section 5 (2) (b) of the Act to ensure procedural safeguards against the misuse of the power under section 5(2).

In *People s Union for Civil Liberties* v. *Union of India*,[62] the Supreme Court held that electoral candidates were under a duty to disclose information about their antecedents, including their assets and liabilities, and could not be protected by any right to privacy when it came to disclosing information which the public had a right to know. Where there are competing interests, the right to privacy of the individual and the right to information of the citizen, in the public interest, the former has to yield to the latter. In any event, the disclosures required to be made by an electoral candidate (pertaining to assets and liabilities as also the criminal records) are matters of public record and there was therefore no infringement of the right to privacy.

*People s Union for Civil Liberties* v. *Union of India*[63] concerned a constitutional challenge to the Prevention of Terrorism Act, 2002 (POTA), *inter alia*, on the ground that section 14 of the Act which mandates the disclosure of information to the police by ordinary people is a violation of

---

61 *Supra* note 12.

62 2004 (4) SCC 299.

63 (2004) 9 SCC 580.

the right to privacy. It was held that privacy is not an absolute right and is, in any event, subservient to the security of the state. Further, the concealment of such information could not be traced to the right to privacy.

The development of privacy jurisprudence in India, despite the progressive attitude of the judiciary in this regard, leaves much to chance. Most modern Constitutions in the world include an express right to privacy, and those that do not, create a legislative framework for its effective protection within their domestic legal systems. India, however, continues to rely on judicial interpretation for affording protection to this fundamental human rights issue recognised by a number of international human rights documents. There is an immediate need for a clear legislative policy in the area of privacy and infringement, in the absence of which the invasion of the personal space will remain largely unchecked. Such a policy is required to include, at the minimum, the unequivocal declaration of privacy as a fundamental right protected by the state against unlawful intervention. The surveillance activities by the state and other actors need to be within the contours of the law, as prescribed by the selfsame document. This document should further incorporate:

i. The circumstances under which such intervention can be justified;

ii. The body competent to authorize such intervention - its structure, powers and functions;

iii. The reasons for the immediate surveillance activity being undertaken;

iv. The methods employed in this exercise, amongst other details.

A clear guideline should be laid down for judicial supervision of the entire process, along with the requirement for submitting a comprehensive report by the government on all such surveillance activities carried out by it.

With the advent of technology, the ever-increasing ambit of surveillance in the pretext of public safety can only be truly delimited with a clear legislative policy. If the state has a serious intention of protecting the rights of its citizens even against itself, as it is obligated to both under international law as well as the Constitution, the current *laissez faire* surveillance scenario needs a complete legislative upheaval. Excessive reliance on the judiciary in the determination of the legality of intervention can hardly be considered prudent. The judicial interpretation at present has no legislative framework for reference, and mere precedents set by previous courts are of limited utility under circumstances where the nature of intervention itself is evolving rapidly. The dearth of legislative will in this respect can prove fatal to the protection of

civil liberties in the country, especially in the case of sensitive rights such as privacy, which are probably more vulnerable than most.

**An attempt to bridge the gap: India s draft privacy bill**[64]

As a response to the requirement for legislative framework for protection of privacy at a national level, the erstwhile UPA-II government prepared a draft bill on the right to privacy in 2014, and upon completion of the draft, sent it to the Attorney General of India for his views and comments. Ironically, the document containing the scathing criticism by the then Attorney General along with his remarks on the plethora of ambiguities within the same was leaked on the internet, prior to it being tabled at the Parliament. This document, amply reprimanded by the Attorney General, was a piece of poor draftsmanship, and included highly uncertain measures for the protection of data security and individual privacy, especially in cases where the government itself was the perpetrator. The considerable public furor over this document led the government redrafting the same, and in early 2014, a third draft was created and subsequently leaked once again, this time to the print media.[65]

The current bill is broader in application, insofar as it extends the right to include all residents of India, and not just citizens, as was mandated by the 2011 draft. It further contains the express acceptance of the right to privacy being a part of article 21, and includes Jammu and Kashmir within its purview, as opposed to the status granted under the previous bill.[66]

A number of new definitions have found a place in the new bill, and alterations have been made to certain others that have been retained from the earlier draft. Significantly, however, the newly included definitions of legitimate purpose and competent authority continue to adhere to the law in force principle, implying that any law passed by a competent legislature may be enough to authorize collection of data from the subject. The changes made to the definition of persons under the bill widen its applicability considerably, and now includes:[67]

---

64 *Available at*: http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011 (last visited on Aug. 8, 2015). This is the only clear analysis of the bill available in the public domain, and hence, the entire study is based on the analyses made in the same.

65 *Ibid*.

66 *Available at*: http://www.medianama.com/2014/03/223-an-analysis-of-the-new-draft-privacy-bill-cis-india/ (last visited on Oct. 8, 2015).

67 Draft Bill on Right to Privacy (leaked) (2011) *available at*: http://cis-india.org/internet-governance/draft-bill-on-right-to-privacy (last visited on Oct. 8, 2015).

> a body corporate, partnership, society, trust, association of persons, government company, government department, urban or local body, or any other officer, agency or instrumentality of the state.

This is one of the salient features of the new bill, which does not preclude the possible governmental excesses. The bill goes further in defining sensitive personal data and covert surveillance , which both quite exhaustively enlist their given domains. The qualified privileges granted within the same also seem *prima facie* reasonable. Among other key definitions amended suggestively to clarify the governmental intent in privacy protection is the removal of the implied consent and CCTV surveillance from the broader definitions accorded earlier.

Under the exceptions to the right to privacy, the 2014 bill retains all but one exception envisaged in the earlier draft, that of detection of crime , which would cast a doubt regarding the possible motive for utilisation of the act, giving way to skepticism about constant governmental surveillance. This apart, the requirement before seeking to exploit these exceptions must be tested for adequacy, proportionality, relevance and with a view to the ultimate objective requirement of such measures adopted.

The 2014 draft limits the instances where privacy concerns may not be entertained, bringing the number down to three, from the original five cases demarcated by the 2011 bill. These are:

i. The processing of data purely for personal or household purposes,

ii. Disclosure of information under the Right to Information Act 2005,

iii. Any other action specifically exempted under the act.

Greater accountability and transparency measures find a place in the new draft, along with provisions relating to choice and consent of individuals being taken on board, which lends an amount of credibility to this deemed legislation.

The following major changes have been made to the 2011 bill:

i. Provisions relating to sensitive personal data: The provisions in the current bill are mostly the same as the earlier one, with regards to the sanction required for the collection of what has been defined in the act as sensitive personal data . The exceptions to this general rule have two new additions in the current bill, one of which is relating to the collection of medical history of policyholder by the insurance company.

The other, more problematic inclusion is: Collected or processed by the Government Intelligence agencies in the interest of the sovereignty, integrity, security or the strategic, scientific or economic interest of India.

The non-requirement of consent in disclosure, for matters pertaining to the workings of investigative agencies of the government, in prevention and investigation of criminal acts, is also an area of concern, mostly because it creates an umbrella protection for governmental excesses and makes it clearly non judiciable, by having this exclusionary clause.

ii. Consensual disclosure of personal information: Both the 2011 and the 2014 bill have the same stipulation which mandates as a norm, the requirement of prior consent before the disclosure of personal information. The exemptions granted in cases where the sharing was:

   a. Part of the documented purpose,

   b. Within exceptions to the right to privacy; or

   c. Authorised by the data protection authority.

The 2014 bill has the additional exception of such information being required by the law or by the intelligence agencies of the government. In consonance with the rest of the bill, this marks out the immunity granted to governmental authorities in collection of personal data, to the extent necessary for the purpose of the activity, in the interest of national security.

iii. Notice in cases of infringement or data loss: The previous bill contained requirements pertaining to the data control authority s duty to publish any information concerning the breach of data to national media, and the current bill has done away with such a provision in favor of the information regarding the breach to be given only to the parties affected, as well as to the authorities concerned.

The previous draft also included a detailed enlistment of the information to be served as a notice to the individual or subject, prior to the collection of the data. This requirement has become two-prong now, and the exact data being collected and its purpose is to be explained only by the data collector. In case there is a change in purpose a further set of information pertaining to such change is to be then notified in accordance with the bill.

iv. Processing of data for anonymity: An interesting addition pertaining to collection of data without prior consent is introduced through the 2014 bill. Under the new scheme, anonymisation of data of personal

nature is mandated, which has to be done within reasonable time after collection. The introduction of this measure is welcome indeed, as greater degree of protection may be expected as a result.

v. Personal data security measures: The levels of protection guaranteed under the 2011 bill are incorporated, and additions made to the list of the nature of breaches that are punishable offences under the same. Despite this, the obligation imposed by the previous document upon the body processing the data to maintain equivalent level of security, is no longer present in the new bill. However, the detailed enumeration is a show of positive intent on the part of the legislators.

vi. International flows of personal data: The exception to the general requirement of this provision, deals with the data collected by law enforcement agencies or intelligence department, and sensitive data in the interest of national security or for purposes of technological or financial interest of countries, is an equally worrisome phenomenon. The clinical intent with which the drafters carve out exceptions to the new bill, which leaves intelligence gathering squarely outside the scope of this bill, does little to demerit the associated skepticism.

The expansion of the powers and functions of the data protection authority under the 2014 bill is a marked improvement, and important new functions are included in them. Regular auditing of personal data to ensure compliance with provisions of the bill, investigating for possible incorporation of international normative standards into working of the statute and the creation of self regulatory framework for corporations as well as a functional approach towards amicable dispute settlement, are key features included in the new draft. This accords significantly greater influence and flexibility to the authority, which will become crucial in its functioning.

The express power to accept complaints of violation or non-compliance under the Act, as well as to investigate them, combined with the authority to issue directives with regards to the same, is another additional responsibility bestowed upon this body.

Offences under the 2014 bill are characterised to penalize more stringently than its older counterpart. Imposition of greater amounts in the form of fine, and the possibility of imprisonment are some of the measures brought in with the view of achieving deterrence of crimes. The bill further stipulates for the minimum rank of the investigating officer, in cases pertaining to violation of right to privacy as envisaged under it.

Under the 2014 bill offences are defined as:

i. Unauthorized interception of communications

ii. Disclosure of intercepted communications

iii. Undertaking unauthorized covert surveillance

iv. Unauthorised use of disclosure of communication data

Having analysed in detail the newly drafted document on the right to privacy, it seems amply clear that the current bill is an improvement over the previous versions. The detailed provisions pertaining to handling, processing and ensuring the security of personal data are appropriate in the management of sensitive information. The definitions of key terms having been introduced, the express elevation of privacy as a fundamental right guaranteed under article 21, the categorical delineation of offences and penalties under the bill as well as the increased punishments, and the specific nature of well-defined exceptions to the generally applicable principles of choice, consent and disclosure upon acceptance, all form salient features of this draft.

The focus of this paper, however, is on the key issue involving the regulation of governmental invasion of privacy, especially through (but not restricted to) the application of technology. The agenda of this bill therefore does little to address that concern, wherein it constructs an impenetrable defense for any governmental activity related to infringement of privacy, addressable only under the writ jurisdiction of law courts. This implies that any investigative agency or law enforcement authority shall be immune from proceedings under the provisions of this act. This position is severely detrimental to the rights of persons subjected to governmental surveillance, for though every other body is held liable for breach and may be prosecuted under the bill, the complete exemption in cases of governmental privacy is cause for serious concern. The adoption of this system institutes an unbridled surveillance regime, without any possibility of ensuring accountability, which in turn raises the question, when the government has been so vociferous in its stance regarding how the same privacy law should apply to both bodies corporate as well as other institutions and individuals alike, why has it kept itself outside the purview of the same? The clich d debate over the primacy of national security does not hold water when, upon analysis the bill reveals that not only can the governmental agencies be exempted when prompted by the zealous fervor in the maintenance of integrity of the nation , but also for any other purpose under the act which can include domestic surveillance measures undertaken for issues of lesser concern as well. The reliance on

the judiciary in defending the rights of the subjects of such surveillance questions the ultimate utility for an act of this nature, since for this category of violations the lacuna continues to exist, despite the operation of the law.

The sheer lack of accountability of investigative authorities gives much room for irresponsible handling of sensitive data, and possible leakage. Such concerns can only be holistically answered upon revisiting this draft and establishing clear guidelines in cases of investigative breach, in the absence of which, it is doubtful whether the said protections granted by this otherwise comprehensive document will succeed in making its subjects any more secure.

## IV Conclusion

With regards to the necessity of surveillance, especially in the post-9/11 scenario, it seems imprudent to argue for a total prohibition of state surveillance. Thus preemptive action, especially in the backdrop of countering terrorism, does indeed play an important role. The contours of surveillance were and are unclear, and a universal definition of privacy remains elusive. However, the question that remains is not whether the state can, within a restricted sphere afford such protection as demanded by the modern individualistic society, but whether the state has any real intention of doing so?

An analysis of the more controversial provisions in the US PATRIOT Act raises this very question. While the increased application of technology by the state is inevitable and so is the consequential rise in cases of alleged breach of the personal sphere, the degree of accountability that ought to accompany such unbridled authority is absent. The lack of any legislative framework in India, where historically, the judiciary has been the chief protector of such human rights as are not expressly mentioned in the Constitution, has been a frequent cause of concern. The initial attempt, in the form of the draft privacy bill, seems to have troubled the waters further. Instead of laying the foundations for protection of individual rights, its gamut of exemptions to governmental authorities in the collection of sensitive personal information seems to question the rationale behind introducing such legislation. Generally perceived to be the means of providing unheard of latitude to governmental agencies in the investigation of acts threatening national integrity, it serves at best as a cushion of immunity in cases of irresponsible handling of sensitive data. A disturbing trend emerges from the similar placement of these nations with regards the issue of privacy protection- one with the most robust, functional and detailed legislative framework; the other without any clear policy in place. The primacy given to national security

over individual liberties seems to be an accepted phenomenon in both these diverse populations.

While the possibility of creating a model surveillance framework, which protects the privacy of individuals without compromising national security, continues to be debated, presently this seems to be the only remaining reconciliation possible between the two apparently conflicting yet necessary ideals. In midst of this debate, attention is hardly paid to significant aspects of the problem at hand- *e.g.*, the efficacy of the governmental measure, or an evaluation of its success, seems to hardly merit discussion. This is odd indeed, considering the enthusiastic rhetoric employed in defending the need for surveillance, no attempts have been made for instituting an evaluative study on the results of the same over the last decade by the governments. Neither has any rationalisation been provided for introducing newer surveillance techniques without the objective appraisal of the existing ones, the inadequacy of which remains to be established, apart from the specter of 9/11 being regularly employed as a shield in all such cases. However, the justification behind each new policy on surveillance needs to be scrutinized under proper judicial supervision, the aims and objects clarified, the quality of the technology assessed- in terms of efficacy in achieving the concerned objects, the degree of intrusion it necessitates and its overall effect on the privacy of individuals. Greater transparency and accountability in carrying out such activities, along with the innovation of novel processes which minimize the loss of anonymity and secrecy of the person, are essential in attempting to bridge the gap between technology, surveillance and the right to privacy.

*Agnidipto Tarafder**

---

* Agnidipto Tarafder, Guest Lecturer, WBNUJS, Kolkata.