Inside the Machine: Constitutionality of India's Surveillance Apparatus

Bedavyasa Mohanty[†]

I. Introduction

On June 6, 2013, The Guardian published a leaked top secret order of the American Foreign Intelligence Surveillance Court (*hereinafter* "FISA Court").[1] The secret court order mandated the production of call details of all Verizon subscribers to the National Security Agency (*hereinafter* "NSA"). This marked the beginning of what has been called the 'biggest intelligence leak in the history of the world'. Few other revelations in the recent past have caused an unprecedented global outrage like that which followed Edward Snowden's leak of NSA's classified documents. The practice of a State monitoring its citizens' activities has been in existence for centuries.[2] Yet, laws governing surveillance and interception of communications have never been subjected to as much debate within the civil society as they have been in the last decade. This upsurge can in part be attributed to an increasing ease in modern communication and, resultantly, a resurgence of what Mill called the "marketplace of ideas"[3] on the internet.[4] In part, however, the growing dialogue is attributable to disenchantment with increasingly oppressive State practices.[5] With rapid growth in technology, there has been an expansion in

---

[†] Junior Fellow, Cyber Initiative, Observer Research Foundation

1 In Re Application of the Federal Bureau of investigation for an order requiring the production of tangible things from Verizon Business Network Services Inc. on behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services, BR 13-80, Foreign Intelligence and Surveillance Court, *available at* https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf

2 *See generally,* L.N. Rangarajan, Kautilya: The Arthashastra 522-524 (1992).

3 John S. Mill, On Liberty (1859).

4 *See generally* Law Reform Commission (Ireland), Report on Privacy: Surveillance and Interception of Communications (1998) *available at* http://www.lawreform.ie/_fileupload/Reports/rPrivacy.htm.

5 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State 6 (2014).

the State's capabilities for supervision over the activities of its citizens. There has, however, not been a complementary augmentation in the safeguards for citizens' rights. Unauthorised interception of communication is indicative of a blatant disregard for the right to privacy available to every person. This becomes doubly relevant in the Indian context where the contours of the law of privacy are still being defined.

The right to privacy, having found no specific protection under any legislation has had to evolve through decades of contradictory pronouncements by Indian courts.[6] However, with every additional buttress for the protection of the right to privacy, there has been the introduction of a rule or law to restrict its application. The Indian government has been putting into operation newer tools for restricting freedoms while the laws governing their application remain archaic and draconian. In a manner reminiscent of the Foucaldian Panopticon,[7] the citizen is made aware of the existence of these tools while the extent of their reach into one's personal life remains shrouded in mystery.

This paper seeks to analyse the nuances of some of these laws and tools that enable the State to keep a constant watch over its citizens' activities. It also attempts to test the validity of the State's surveillance powers against the principles of liberty and justice enshrined in the Indian Constitution. In doing so, the author aims to challenge the archaic foundations of Indian surveillance laws while drawing attention to areas that are in need of re-examination or, in some cases, complete overhaul. Part II of the paper is a brief exposition of the various laws and rules currently in effect that enable the State to intercept communications. This part aims to highlight the systemic shortcomings that are common to all legislations pertaining to surveillance. Part III traces the development of these laws across modern history in an attempt to unearth and examine the bases of the power of interception. This exercise aims to bring to light the severe lack of legislative discourse that surveillance laws have been subjected to in India. It also seeks to highlight the dire necessity of immediate legislative re-examination of these laws. Part IV attempts to explore the incongruity between the powers of interception of communications and the fundamental freedoms assured in the Constitution.

---

[6] For the development of the right to privacy in India, *see generally Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295; *R.M. Malkani* v. *State of Maharashtra*, (1973) 1 SCC 471 : AIR 1973 SC 157; *Gobind* v. *State of M.P.*, (1975) 2 SCC 148 : AIR 1975 SC 1378; *R. Rajagopal* v. *State of T.N.*, (1994) 6 SCC 632 : AIR 1995 SC 264; *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568; *Naz Foundation* v. *Govt. of NCT of Delhi*, 2009 SCC OnLine Del 1762 : (2009) 160 DLT 277; *Selvi* v. *State of Karnataka*, (2010) 7 SCC 263.

[7] Michel Foucalt, Discipline and Punish: The Birth of the Prison 201 (1975).

It contends that surveillance in its current form may not constitute a reasonable restriction envisaged under Article 19(2) of the Constitution. Part V examines the unfeasibility in implementation of these laws and explores their shortcomings that inhibit the actualisation of constitutional goals. Part VI looks at similar laws and rules in force in other developing and developed nations. These include countries that have traditionally been proactive in delineating the contours of privacy laws and countries that have followed a comparable timeline in democratic development since their independence in the 20th Century. This part highlights surveillance practices followed in these countries that can feasibly be adapted to an Indian context to make our laws more progressive. The scope of this paper is limited to the examination of the substantive principles allowing the State to intercept communications and it does not attempt an in-depth analysis of the rules of procedure governing the same. This is due to the fact that procedural aspects of surveillance laws have attained relative clarity after the judgment in People's Union for Civil Liberties v. Union of India.[8]

II. Legislations governing surveillance

Any attempt at evaluating the surveillance regime in India must begin with an assessment of laws that empower the State to intercept communications. Communication in the modern context predominantly relates to messages transmitted via the telecommunication networks.[9] All licensing agreements entered into between the State and internet/telecommunications service providers contain provisions which enable the State to intercept users' communications.[10] However, the fountainhead from which the State derives its powers of interception is the triumvirate of the Indian Telegraph Act, 1885, the Indian Post Office Act, 1898 and the Information Technology Act, 2000. These legislations along with various rules drafted thereunder serve as the enabling statutes for State surveillance. This part details the provisions that authorise interception of communications and discusses the factors common to all three laws.

---

[8] *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568.

[9] Teodor Serbanescu, Personal Communication *available at* https://www.wpi.edu/Pubs/E-project/Available/E-project-090311-151245/unrestricted/Personal_Communication_IQP.pdf (Last visited on Aug. 18, 2016).

[10] *See* Clause 41.1, Unified Access Service License, Department of Telecommunication, Ministry of Information and Broadcasting, *available at* http://www.dot.gov.in/sites/default/files/Unified%20Licence.pdf (Last visited on Aug. 18, 2016); Clause 39.12 Unified Licence, Department of Telecommunication, Ministry of Information and Broadcasting, *available at* http://www.dot.gov.in/sites/default/files/Unified%20Licence.pdf (Last visited on Aug. 18, 2016).

A. Indian Telegraph Act, 1885

For the surveillance of telephone networks, the Indian Telegraph Act, 1885 (*hereinafter* "the Act") serves as the primary enabling statute. The term "telegraph" as defined under §3(1AA) of the Act is broad and expansive. It includes "any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electromagnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means."[11] This is a "broad and future-proof definition"[12] which brings all communication devices into the ambit of the Act.

§5 of the Act authorises the State to intercept and detain telegraphs and telegraphic communication. It also lays down conditions under which the power of interception can be exercised. §5(2) which enables interception of telegraphic articles can only be used on the occurrence of a "public emergency" or in the interest of "public safety". Further, it must also be established that the interception is necessary or expedient in the interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence. The power under §5 has been vested with an administrative official authorised by the Central or State Government.

B. Rule 419A, Indian Telegraph Rules, 1951

Rule 419A of the Indian Telegraph Rules lays down detailed procedure for intercepting communications. Under sub-rule (1) an order for lawful interception must normally be passed by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. Under exigent circumstances though, the power of interception may also be used by an officer not below the rank of a joint secretary who has been authorised by the government. Rule 419A clarifies that an order of interception may only be passed where other methods of obtaining the information have been tried and have failed. The Rule stipulates that any order permitting tapping of communication would lapse (unless renewed) in two months. In no case would tapping be permissible beyond 180 days. The Rule further requires all records of tapping to

---

[11] Indian Telegraph Act, 1885, §3 (1AA).

[12] Software Freedom Law Centre, India's Surveillance State(2014), *available at* http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf (Last visited on Aug. 18, 2016).

be destroyed after a period of two months from the lapse of the period of interception.

C. Indian Post Office Act, 1898

§26 of the Indian Post Office Act is analogous to §5 of the Indian Telegraph Act and governs the interception of postal communication. Not unlike the Telegraph Act, the power of interception of postal articles is also vested with an executive authority authorised by the government to do so. Most modern communication takes place over the internet and telecommunication networks. Due to this reason, interception provisions under the Post Office Act have been rendered all but irrelevant in the 21st Century. However in the hundred sixteen years of its existence the Act has been the subject of many controversial claims of being used for political subversion.[13]

D. Information Technology Act, 2000

Drafted in the year 2000, the Information Technology Act is the first legislation that governs and regulates information transmitted via computer networks. §69 of the Act is also modelled extensively along the lines of §5(2) of the Telegraph Act. §69, however, does away with the requirements of the existence of a public emergency and interest of public safety. Instead it adds defence of India and investigation of any offence as additional grounds under which communication may be intercepted. Further, §69 also imposes an obligation on private entities, like internet service providers to render assistance to intercepting authorities failing which, they may be punished with imprisonment up to seven years.

E. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules are similar to the Rule 419A of the Indian Telegraph Rules. The only major distinction between the two sets of rules is that while Rule 419A allows interception of communication relating to a person or a class of persons, the IT Rules additionally allow

---

[13] Prabhu Chawla, *Postal censorship: Storm in the letterbox*, India Today, Aug. 31, 1981, *available at* http://indiatoday.intoday.in/story/delhi-police-intercept-read-and-re-post-mails-of-264-persons/1/402130.html (an examination of the list of persons whose communications were intercepted reveals that the majority of them were people who were considered political opponents of Mrs. Indira Gandhi) (Last visited on Aug. 18, 2016).

interception of communication relating to a subject matter. The relevance of this departure is discussed in the subsequent sections of this paper.

III. Historical Antecedent of §5(2)

Surveillance for gathering and controlling information has long been a prevalent practice among Indian statesmen. The Arthashastra speaks of the ruler surreptitiously gathering intelligence for stifling dissent and identifying rebels.[14] Other historic texts evidence the practice of installing ambassadors and hermits for gathering intelligence from foreign lands and communal places respectively.[15] The Mughals are credited with being among the first to institutionalise this system. They favoured gathering political intelligence through a comprehensive network of post offices called *dakchaukis* that were manned by a State official.[16] These early attempts at an institutionalised system of intelligence gathering, however, were not meant to create a police State. The primary motivation for intercepting communications in pre-colonial India was to detect "moral transgressions among their officers and the oppression of the weak by the powerful."[17] The rulers also used this information to obtain practical insights into the financial conditions of their taxpayers.[18] In essence, surveillance systems in ancient and modern India were used not for prevention and detection of crime. They were meant to ensure better administration and better allocation of resources.

Evidence suggests that the practice of information gathering through interception of communication carried over to Colonial India as well.[19] However, the British interest in observing and controlling the flow of information within India was different from the rulers that came before them. The *raison d'être* behind surveillance under the Crown was limited largely to protection of military intelligence and dissemination of British propaganda.[20] This was accomplished by the deputation of two army officials as the Chief Telegraph Censor and the Chief Postal Censor under the Director

---

[14] Wendy Doniger & Brian K. Smith, The Laws of Manu 225-226(1991).
[15] Kamandaki, The Nitisara (Rajendra L. Mitra ed., 1982).
[16] M.Z. Siddiqi, *The Intelligence Services under the Mughals*,*in* Medieval India: A Miscellany 253, 260 (1972).
[17] C.A. Bayly, Empire and Information : Intelligence Gathering and Social Communication in India, 1780-1870 10 (1997).
[18] *Id*.at 13.
[19] *See* Sir William Muir , Records of the Intelligence Department of the government of the North-West provinces of India during the Mutiny of 1857(1902).
[20] *Id*.

of Military Operations and Intelligence.[21] It is during this time that earliest versions of the laws governing surveillance were first drafted. In one form or another, these laws have managed to survive into present day and continue to guide the State in exercising control over its citizens' speech.

Modern forms of surveillance trace their origins to §5 of the Indian Telegraph Act, 1885. It was the first legislation that sought to lay down the conditions for conducting surveillance and intercepting communications. While the substantive conditions precedent for intercepting communications remained the same, the Act in its original form lacked any safeguards against misuse of the provisions. §5(1) of the Act authorised the Governor General in Council or an officer authorised by him to take temporary possession of or intercept and detain any telegraphic communication on the occurrence of a public emergency or in the interest of public safety.[22] Unlike the present Telegraph Act, however, there was no requirement for recording written reasons for intercepting the communication. Moreover, §5(2) of the Act clarified that if there was any doubt about the existence of a public emergency or a threat to public safety a "certificate signed by the Secretary to the Government of India or to the Local Government would be conclusive proof upon that point."[23] This provision barred judicial review of an action taken by a delegated administrative official of the government under the Act.

The next legislation that sought to further expand the powers of the State for intercepting communications was the Indian Post Office Act of 1898. Drafted thirteen years after the enactment of the Telegraph Act, it borrowed heavily from the language of §5. The Post Office Act under §26(1), however, included one additional safeguard that an order for interception had to be made in writing. The Select Committee instituted to examine the *vires* of the Post Office Bill had differing opinions regarding the powers granted to the government under the Bill.[24] Shri P. Ananda Charlu, a member of the Select Committee, noted his dissent highlighting the arbitrariness of the power granted to the government under the Bill. Charlu, in particular, pointed out that the bill lacked a provision mandating that an individual be notified if his/her communication was intercepted but no charges pressed.

---

[21] Constitution of Central Board of Information: Thorne's report on war-time control of press, broadcasting, films and publicity(1939) *in* Sanjoy Bhattacharya, *British Military Information Management Techniques and the South Asian Soldier: Eastern India during the Second World War*, 34 (2) Modern Asian Studies 483-510 (2000).

[22] §5(1), Unamended Indian Telegraph Act, 1885 adopted by the Governor General in Council on July 22, 1885 *available at* http://lawmin.nic.in/legislative/textofcentralacts/1885.pdf (Last visited on Aug. 18, 2016).

[23] *Id*. at §5(2).

[24] Gazette of India, March 12, 1898, part V, *in* Law Commission Report No. 38 on the Indian Post Office Act.

He noted that disclosures regarding interception may act as a deterrent to future offenders. Consequently, he went on to suggest that the lack thereof tilted the balance heavily in favour of the government and against the public. He also cautioned that the lack of safeguards would render the Bill open to misuse by a corrupt government in the future.[25] Shri Bisambar Nath, another Indian member of the Council, also noted his apprehensions by suggesting that without due clarity regarding the conditions for existence of a public emergency, the power prescribed by the Bill was arbitrary.[26] The Bill was, nevertheless, passed without any amendments or the addition of any safeguards.

The Telegraph Act and the Post Office Act (*hereinafter* "the Acts") continued to remain in operation even after the country gained independence. During this time there was little to no recorded discourse on the lack of safeguards under the Acts except a Press Laws Enquiry Committee in 1947. The Committee only recommended that §§26 and 5 of the respective Acts should be amended so that actions and orders of subordinate officers are reported to and reviewed by responsible ministers of the government.[27] The first comprehensive examination of the Acts was undertaken by the Law Commission in its 38th Report on the Indian Post Office Act in 1968. The Law Commission was of the opinion that insofar as §26 of the Post Office Act intercepted or detained one's communication, it was a restriction on the freedom of speech and expression guaranteed under Article 19 of the Constitution.[28] Therefore, for interception to be permissible under §26, the rationale for such interception must be within the ambit of limitations prescribed under Article 19(2). Once again the Law Commission voiced concerns regarding the vagueness of the term 'public emergency'. It noted that if the emergency was not of such a character as to threaten public order or the security of the State, then it would go beyond the restrictions mentioned in the Constitution.[29] To that end, the Law Commission proposed an amendment to §26 of the Post Office Act and §5 of the Telegraph Act. It suggested that an order for interception must only be passed if it was "required in the interests of the security of the State, friendly relations with foreign States or public order or for preventing the incitement to the commission of any offence."[30] This, in the Law

---

[25] Gazette of India, March 26, 1898, part VI, 285-287, *in* Law Commission Report No. 38 on the Indian Post Office Act.

[26] *Id.*

[27] Virendra Kumar, *Report of the Press Laws Enquiry Committee, 1947* in Committees and Commissions in India 1947-54, Volume I (2004).

[28] Law Commission of India, 38thLaw Commission Report ¶83 (1968).

[29] *Id.*

[30] Law Commission of India, *supra* note 28 at ¶93.

Commission's opinion, would go a long way in making the Acts compatible with the Constitution.

The Commission also considered §26(2) of the Post Office Act that barred judicial review after an administrative determination of the need for interception. The Commission found this provision to be wholly unconstitutional. It recorded that *vires* of an interference with freedom of expression had to be examined on the basis of whether the interference fell afoul of the limitations set out in the Constitution.[31] This determination could only be done by a court of law. The Commission therefore directed the government to omit the provision from the Acts.

Following the Law Commission's recommendation to amend the Telegraph Act, the legislature passed the Telegraph (Amendment) Act, 1972. The amendment repealed the erstwhile §§26(2) and 5(2) of the Acts. Orders of interception were now subject to judicial review.[32] Additionally, the legislature sought to bring the Acts within the ambit of restrictions laid down under Article 19(2). Following the Law Commission's recommendations, many of the restrictions listed under Article 19(2) were imported into §5(2) of the Telegraph Act.[33] It may be interesting to note here that the Law Commission had recommended the addition of a provision that authorised interception only if it was *required* under the conditions set out in Article 19(2).[34] This meant that interception orders could be passed only if it was absolutely necessary to do so. However, the provisions were amended to provide that communications could be intercepted if it was 'necessary or expedient'.[35] Thus, an additional dimension of vagueness *i.e.* 'expediency' was included in the already ambiguous provisions for interception. The consequences of this ambiguity in drafting have been discussed in the later parts of this paper. This paper, however, is not the first time that this lack of legislative clarity has been called into question.

The parliamentary debates surrounding the amendment reflected grave concerns regarding the arbitrariness in conferring powers, and ambiguity in language of the Act. The tenor of discussion reflected that the powers vested

---

31 Law Commission of India, *supra* note 28 at ¶86.

32 The Indian Telegraph (Amendment) Act, 1972, §5.

33 The amendment mandated that in addition to the existence of a public emergency and a threat to public safety, the State would have to be satisfied that it was necessary or expedient in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence to pass an order of interception.

34 Law Commission of India, *supra* note 28.

35 The Indian Telegraph (Amendment) Act, 1972, §5(1).

in the State under §5(2) were largely considered "excessive"[36] when a proclamation of emergency was not in effect. Concerns were also voiced regarding the lack of definition of the terms used in the Act.[37] It was also feared that the provisions may cause difficulties in centre-state relationships. A conflict of opinion could arise between the government at the centre and the government at the state. In such a case the central government, which controls the Telegraph Department, would be in a position to create hindrances in dissemination of information from the state to other parts of the country.[38] In the Rajya Sabha it was pointed out that terms like public emergency had not been defined in the Constitution. Therefore, it was not a reasonable restriction on freedom of speech and expression.[39] It was also cautioned that even the legitimate use of public emergency for interception left the provision open to misuse. While public emergency could be construed to be a special circumstance requiring exigent action, protection of public safety was a continuing concern. Therefore, even in cases where an emergent situation did not exist, interception orders could be passed by claiming that it was in the interest of public safety.[40]

All of the aforementioned concerns raised in the parliament were either unaddressed or brushed aside as trivial by Shri H.N. Bahuguna, the then Union Minister of Communications. He insisted that terms like public emergency had been derived from within the Constitution and were therefore valid restrictions on fundamental rights.[41] In response to the potential misuse of the provisions, the Hon'ble Minister claimed that there had been no reported cases of misuse and therefore it was unlikely that it would happen in the future.[42] What the Hon'ble Minister failed to acknowledge, however, was that without adequate safeguards and any provision for post-interception disclosures, no cases of misuse would ever be brought into the public eye. Moreover, even if it were found to be true that no misuse of §5(2) had occurred till 1972, this fact would not in itself preclude the possibility of misuse of the Section in the future. The Hon'ble Minister's claims were therefore a falsification of existing facts at worst or a moral high ground fallacy at best. Thus, despite numerous misgivings regarding the powers being

---

[36] Parliamentary Debates, Lok Sabha, 09 August 1972, 218 (Shri Dinen Bhattacharyya, Member of Parliament) (Ind.).

[37] *Id.* at 219.

[38] Parliamentary Debates, *supra* note 36 at 219.

[39] Parliamentary Debates, Rajya Sabha, 31 July 1972, 268 (Shri Salil Kumar Ganguly, Member of Parliament) (Ind.).

[40] *Id.* at 264.

[41] Parliamentary Debates, Lok Sabha, 09 August 1972, 228 (Shri H.N. Bahuguna, Minister of Communications) (Ind.).

[42] Parliamentary Debates, Rajya Sabha, 31 July 1972, 266 (Shri H.N. Bahuguna, Minister of Communications) (Ind.).

vested under the Act, the government Bill was passed in both the houses of the Parliament. For nearly two decades thereafter, there are no records of any judicial or legislative consideration of the ambiguity in surveillance laws. What is clear, however, is that during this time the interception provisions were used extensively by the government.[43] Often, such orders of interception were alleged to have been passed unjustly and in furtherance of political motives rather than in public interest.[44] It therefore became apparent that surveillance powers of the State could no longer be allowed to operate unbridled and without due procedure.

The year 1997 proved to be a watershed moment in the history of surveillance law. That year a division bench of the Supreme Court passed an order in People's Union for Civil Liberties v. Union of India (*hereinafter* "PUCL")[45] and added a slew of procedural safeguards to interception under §5(2). In PUCL, a PIL was filed challenging the constitutionality of §5 of the Telegraph Act. The contention of the petitioner was that there had been no procedural rules laid down under §7(2)(b) of the Act which gives the State the power to lay down precautions against improper interception and disclosure of messages. This had led to rampant misuse of the power of interception. The Court affirmed that tapping of telephones was indeed a breach of privacy and a restriction on free speech. It was therefore a restriction on rights guaranteed under both Articles 21 and 19 of the Constitution. Any order of interception would be illegal if it was not passed as per the due procedure of law. To that end, the Supreme Court suggested procedural safeguards to make the process of interception more transparent and uniform. It also suggested the setting up of a review committee to analyse every order of interception on the basis of certain criteria. As a result of this decision, the legislature included Rule 419A to the Indian Telegraph Rules, 1951 in the year 2007. Rule 419A reiterates the suggestions that were given in PUCL. The judgment in PUCL streamlined to a great extent the procedure for conducting surveillance. However, the substantive infirmities in the law, that had been pointed out time and again, fell through the cracks of this historic judgment. Concerns such as the excessiveness of powers granted to administrative authorities and lack of oversight etc. have not yet been considered by Indian courts. The next part of this paper draws attention to some of these substantive infirmities.

---

[43] *See generally*, People's Union for Civil Liberties, *Mail and Telephone Censorship*(1982) *available at* http://www.pucl.org/from-archives/Media/mail-phone.htm(A chronicle of the various allegations of misuse of the interception provisions by the government and the resultant protests against this misuse.) (Last visited on Aug. 18, 2016).

[44] Chawla, *supra* note 13.

[45] *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568, ¶ 35.

IV. Constitutionality of §5(2)

Any Act that restricts the fundamental rights guaranteed to a citizen must be in accordance with procedure validly established by the law. Such procedure must be "fair, just and reasonable and non-arbitrary, non-fanciful or non-oppressive."[46] The contention in PUCL was with regards to the lack of adequate procedure for conducting surveillance. However, the Constitutional *vires* of §5(2) was not "seriously challenged."[47] So far, there has been no judicial determination of whether the conditions for authorising surveillance are arbitrary or oppressive. Therefore, while the procedure for conducting surveillance has been detailed with relative clarity, the prerequisites for authorisation of surveillance are yet to be explicated.

Authorisation for interception is still granted on the basis of conditions that had been laid down over a century ago. §5(2) outlines a two-tiered test that must be satisfied for the interception of telegraphs. The first-tier consists of *sine qua non*[48] in the form of an 'occurrence of public emergency' or 'in the interest of public safety'. An officer passing an order must first establish the existence of either one of the two conditions. Thereafter he must undertake an examination of whether it is necessary or expedient in the interest of public order or national security to pass an order of interception. There are, however, no objective criteria prescribed in the Acts on the basis of which an authority is meant to arrive at these conclusions. He must, in that case, necessarily arrive at these findings on a discretionary assessment of the facts and circumstances. The power under the Act has not been vested in a judicial authority but an administrative one. If the power had been vested in a judicial or Constitutional authority, there would have been a presumption of legitimate use of the power. For instance, in Babulal Parate v. State of Maharashtra, it was held that when a power is conferred on a judicial authority it can be assumed that the power would be exercised legitimately and honestly.[49] A similar decision regarding a Constitutional authority was arrived at in Accountant General v. S. Doraiswamy.[50] Under the Telegraph and Post Office Acts, the power to suspend a person's fundamental rights has been left to the discretionary assessment of an administrative official.

---

[46] *Maneka Gandhi* v. *Union of India*, (1978) 1 SCC 248; *State of Maharashtra* v. *Bharat Shanti Lal Shah*, (2008) 13 SCC 5.

[47] *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568 ¶ 34.

[48] *Hukam Chand Shyam Lal* v. *Union of India*, (1976) 2 SCC 128.

[49] *Babulal Parate* v. *State of Maharashtra*, AIR 1961 SC 884 : (1961) 3 SCR 423.

[50] *Accountant General* v. *S. Doraiswamy*, (1981) 4 SCC 93 : (1981) 2 SCR 155. (It was held that the Comptroller and Auditor General being a high ranking Constitutional authority can be expected to act without arbitrariness and a discretionary power conferred on him does not violate the principle against excessive delegation.).

Some of the specific aspects of §5 that are vague and indeterminate are discussed herein.

A. On the Occurrence of Public Emergency

The term 'public emergency' has been in operation within the Telegraph Act since its very inception. It has remained the focal point of controversy relating to the arbitrariness of the interception powers. The major concern surrounding 'public emergency' is that the term has not been defined by the legislature.[51] Hence the determination of whether public emergency exists can often fall to a delegated administrative official. The term 'public emergency' and all orders for interception arising out of it shall be deemed to be arbitrary unless it can hold up against a test of constitutionality. In other words, for public emergency to continue to remain in operation in the Act, it must be established that the existence of public emergency is one of the conditions envisaged in the Constitution for restricting fundamental rights. Questions regarding the elusive definition of public emergency were raised during the passing of the Indian Telegraph (Amendment) Act, 1972. In response, it was claimed in the Parliament that the basis of the terms appearing in the Act could be located within the Constitution.[52] Thus, public emergency could be a valid ground for restricting freedom of speech and expression. This, however, is not true. Although the Constitution uses the term 'emergency', it does not mention the phrase 'public emergency'. For Bahuguna's claims to find any credence, public emergency would have to be taken to mean the same as a proclamation of emergency or any other form of emergency mentioned in the Constitution. Both, the Second Press Commission in 1952 and the Law Commission in its 38th Report in 1968 attempted to discern the meaning of 'public emergency' but failed to arrive at an exhaustive definition. The Law Commission acknowledged that the phrase public emergency is very broad and §§26 and 5 of the Acts contemplate interception of communications during peaceful times as well.[53] The Press Commission clarified that public emergency need not be confined to an emergency arising out of war or external aggression. It may arise locally and yet it may have repercussions in other parts of the country.[54] Moreover, the Indian Telegraph Act was drafted nearly six decades before the Constitution of India was brought into force. It is inconceivable to imagine that a law drafted in the 19th century was meant to be synonymous with a proclamation of emergency. Further, conceiving

---

[51] *Communist Party of India (Marxist)* v. *Commr. of Police*, 1994 SCC OnLine Bom 281 : AIR 1995 Bom 136.

[52] Parliamentary Debates, *supra* note 41.

[53] Law Commission of India, *supra* note 28 at 97, ¶1067.

[54] Second Press Commission, Commission Report 62 (1952).

public emergency as a proclamation of emergency may even create additional barriers in the implementation of the law. By way of illustration, let us consider the argument that public emergency is the same as a proclamation of emergency. Then, any requests by law enforcement agencies to intercept communications would require them to establish that a state of emergency exists. This is an extremely high threshold to meet. Instead, law enforcement agencies would find it easier to establish that public safety is threatened and requires the interception of communications. Over time this would cause the phrase 'public emergency' to become redundant. Public emergency therefore cannot be conflated with a proclamation of emergency.

The only guidance to the possible meaning of 'public emergency' came from the Supreme Court in Hukam Chand Shyam Lal v. Union of India (*hereinafter* "Hukam Chand").[55] Therein, a four judge bench of the Supreme Court defined 'public emergency' as a situation "which raises problems concerning the interest of the public safety, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or the prevention of incitement to the commission of an offence."[56] This definition seemingly brings public emergency into the ambit of the restrictions laid down under Article 19(2) of the Constitution. In reality, though, it does not lend any clarity to the indeterminacy surrounding the term.

Firstly, both public emergency and public safety are envisaged as conditions precedent to the exercise of power under §5. In this regard the Court was correct in holding that the two phrases must take their colour off each other. But interpreting public emergency as a situation that must necessarily implicate public safety does not assist in delineation of the term. Instead, it renders the term 'public emergency' redundant. The fact that the two terms have been separately included in the Act means that they must necessarily refer to two distinct situations.[57] Granted, that situations may arise where both public emergency and public safety overlap; however there must necessarily be situations where a public emergency has arisen but public safety is not threatened. By way of illustration, an imminent strike that may cease operation of transportation services may be an emergent situation affecting the public while not necessarily threatening the safety of the public. This would then qualify as a public emergency but would not implicate public safety.

---

[55] *Hukam Chand Shyam Lal* v. *Union of India*, (1976) 1 SCC 128.
[56] *Hukam Chand Shyam Lal* v. *Union of India*, (1976) 1 SCC 128.
[57] Law Commission of India, *supra* note 28 at 92.

Secondly, the Act envisages public emergency as a *sine qua non* before a threat to sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order exists. The Supreme Court's interpretation seeks to define public emergency as a situation where public order, sovereignty and security of the State are already threatened. This is a cyclic interpretation of §5 where it is difficult to understand whether a threat to public order and security create a condition of public emergency or vice versa.

There are therefore no objective criteria against which the existence of public emergency can be measured. Thus, the question of the existence of a public emergency is left to the subjective determination of a delegated official. The question that arises at this juncture is whether the subjective assessment by a delegated administrative official is sufficient for the suspension of fundamental rights. A similar question arose before the House of Lords in Liversidge v. Anderson.[58] The case examined the *vires* of an Act that vested an administrative authority with the power to detain a person if there was reasonable cause to believe that the person was of hostile origin. Lord Atkin in his dissenting opinion weighed in on the conditions set out for the power in question to be exercised. Relying on Greene v. Secy. of State for Home Affairs,[59] he was of the opinion that the precondition of "a reasonable cause to believe" was one requiring subjective determination and not an objective one. Further, the power that was meant to be vested in the administrative official was a conditional one. However, by allowing an administrative authority himself to determine whether he was entitled to use his power, the law had the effect of vesting in him an absolute authority instead of a conditional one. In such cases, the only protection available against misuse of such power was the belief that the official was acting in good faith. This proposition was unacceptable to Lord Atkin. He opined that any law that lays down preconditions for the exercise of a certain power but lacks objective criteria to test whether the preconditions have been met is unsustainable. Although, Lord Atkin's judgment formed the dissenting opinion, it has since emerged as the more logically defensible position.[60]

---

[58] *Liversidge* v. *Anderson*, 1942 AC 206.

[59] *Greene* v. *Secy. of State for Home Affairs*, 1942 AC 284.

[60] *See Lord Diplock in IRC* v *Rossminster Ltd.*, 1980 AC 952, at 1011 : (1980) 2 WLR 1 "the time has come to acknowledge openly that the majority of this *House in Liversidge* v. *Anderson* were expediently and, at that time, perhaps, excusably, wrong and the dissenting speech of Lord Atkin was right"; *Also See ADM, Jabalpur* v. *Shivakant Shukla*, (1976) 2 SCC 521 : AIR 1976 SC 1207.

A similar position was also taken by the Supreme Court in State of M.P. v. Baldeo Prasad.[61] The case dealt with the constitutionality of the Central Provinces and Berar Goondas Act, 1946 and the lack of the definition of *Goondas* under the Act. While deeming the statute as unconstitutional, the Court held that a statute must provide adequate safeguards for the protection of innocent citizens. It must also require the administrative authority to be satisfied as to the existence of the conditions precedent laid down in the statute before making an order. If the statute failed to do so in respect of any condition precedent, then the law suffered from an infirmity and was liable to be struck down as invalid. Similarly, public emergency has not been defined under the Telegraph Act. Moreover, the legislature has also failed to lay down any objective criteria that may guide the administrative authority in coming to a conclusion regarding the existence of public emergency. This view also finds support from the findings of the Second Press Commission. The Press Commission acknowledged the vague nature of public emergency and its potential to be misused by delegated officials. It was of the opinion that the appropriate government should declare the existence of a public emergency by a notification warranting the exercise of the power under §5. Only after the issue of such a notification would the delegated authority be able to exercise the power of withholding telegraphic messages.[62] This, however, is not a practical solution. In exigent cases where an order of interception may need to be urgently issued, it may be impossible to obtain a declaration of public emergency from the appropriate government. A more plausible solution may be a clearer definition of the term.

It is now evident that the definition of 'public emergency' is vague at best. Any law that seeks to restrict the fundamental rights of individuals must be fair, just, reasonable and non-arbitrary.[63]As the law stands today, the determination of a condition of public emergency is left to the arbitrary decision of a delegated authority. Hence, the occurrence of a public emergency is not a valid ground for interception of communications and consequently for restricting freedom of speech and expression. In its current form, it is therefore *ultra vires* the constitution and liable to be struck down.

Unfortunately, Indian laws provide little guidance in discerning a non-exclusionary meaning of the term. The only statute that uses the term 'public emergency', not in the context of surveillance, is the Factories Act, 1948.[64] This 'public emergency', however, is limited only to an emergency whereby

---

[61] *State of M.P.* v. *Baldeo Prasad*, AIR 1961 SC 293.
[62] Second Press Commission, *supra* note 54 at 62.
[63] *Maneka Gandhi* v. *Union of India*, (1978) 1 SCC 248.
[64] Factories Act, 1948, §5.

the security of India is threatened, by war or external aggression or internal disturbance.[65] The Supreme Court has already held that public emergency cannot be equated with any other form of emergency.[66] Hence, other statutes using the term 'emergency'[67] may not provide any guidance in the interpretation of this term. It may, therefore, be necessary to look beyond the Indian legal system to understand what the phrase means. In the context of protection of human rights, the European Court of Human Rights (*hereinafter* "ECtHR") has attempted to define 'public emergency'. In Lawless v. Ireland,[68] it defined the phrase as "an exceptional situation of crisis or emergency which affects the whole population and constitutes a threat to the organised life of the community of which the State is composed."[69] This definition was further developed by the ECtHR in the Greek Case.[70] In that matter the Court further clarified the term to having been said to exist only when a threat is actual or imminent and the effects of emergency involve the whole nation. Further, the continuance of the organised life of the community must be threatened for a declaration of public emergency. It was also held that the crisis or danger must be so exceptional that the normal measures or restrictions, permitted by European Convention on Human Rights for the maintenance of public safety, health and order, must have proven to be inadequate.[71] Admittedly, the pronouncements by the ECtHR are in the context of derogation of national responsibility in relation to human rights under emergent circumstances. These definitions therefore cannot be directly imported into Indian surveillance laws.

When delineating a power that is exercised for regular law enforcement, the Act cannot rely on a definition that necessitates the existence of 'exceptional' social conditions. Instead, Indian courts must strive to arrive at a more balanced definition. It is entirely possible to define public emergency under the Acts without relying on principles of public order or public safety. A good starting point can be the classification of criminal acts as those that threaten national security and those that do not. A near inclusive list of threats to national security could then be said to cause a public emergency,

---

[65] Explanation to §5, Factories Act, 1948.

[66] *Hukam Chand Shyam Lal* v. *Union of India*, (1976) 2 SCC 128.

[67] *See for example*, §11(2) of the Official Secrets Act, 1923 and §4A of the Indian Tariff Act, 1934

[68] *Lawless* v. *Ireland*, 1961 ECHR 2.

[69] *Lawless* v. *Ireland*, 1961 ECHR 2 ¶28.

[70] The Greek Case, (1969) 12 YECHR (Application No. 3321/67, *Denmark* v. *Greece*; No. 3322/67, *Norway* v. *Greece*; No. 3323/67, *Sweden* v. *Greece*; No. 3344 *Netherlands* v. *Greece*).

[71] Tahmina Karimova, Derogation from Human Rights Treaties in Situations of Emergency *available at* http://www.geneva-academy.ch/RULAC/derogation_from_human_rights_treaties_in_situations_of_emergency.php (Last visited on Aug. 18, 2016).

while everything else would only threaten public safety. Any such classification must then necessarily be followed by different rules of procedure for reacting to the different classes of threats. In fact, such a distinction may be the only thing that helps §5(2) of the Telegraph Act retain its constitutionality when the matter comes for consideration before the courts.

B. Expedient in the Interest of National Security and Public order

Another point of concern that raises doubts about the Constitutionality of §5 of the Telegraph act is the use of the word 'expedient' for authorising an interception. The Law Commission in its 38th Report suggested that surveillance should be undertaken only if it was necessary under one of the grounds listed in Article 19(2).[72] The legislature however amended the Act in a manner so that communications could be intercepted if it was either necessary or expedient to do so. The meaning of the term expedient is not *res integra*. It has been defined to mean something that is apt or suitable to the end in view.[73] It can be also taken to mean something that is either practical and efficient or advantageous.[74] In other circumstances it can be understood as a device "characterised by mere utility rather than principle, conducive to special advantage rather than to what is universally right."[75]

In light of these definitions, it is fairly simple to conclude that the burden for determining an act of interception as expedient is much lower than determining it as necessary. This essentially means that the State can choose to intercept a person's communication if it finds such interception an efficient means of obtaining communication. The term 'expedient' therefore, *prima facie* seems at odds with Rule 419-A(3) of the Indian Telegraph Rules, 1951. Rule 419-A(3) States that an administrative authority shall only pass an order of interception when it is not possible to obtain the information by any other reasonable means. However, the use of the term 'expedient' gives the authority the power to intercept communication even on the mere satisfaction that it is efficient or advantageous to do so. The power to determine whether it is expedient in the interest of public order, security and sovereignty of the State to intercept and detain communications therefore seems arbitrary and falls afoul of the constitutional principles of just, fair and non-arbitrary.

---

[72] Law Commission of India, *supra* note 28.
[73] Wharton's Concise Law Dictionary (2011).
[74] *Hotel Sea Gull* v. *State of W.B.*, (2002) 4 SCC 1, 13.
[75] *State of Gujarat* v. *Jamnadas G. Pabri*, (1975) 1 SCC 138.

V. Difficulties with standards of enforcement

The surveillance set up under the Telegraph Act and Post Office Act suffers not only from substantive infirmities but also from institutional ones. One of the imminent concerns is regarding the severe lack of oversight of the surveillance set up. In accordance with the court's direction in PUCL, Rule 419-A(16) provides for the establishment of a three member Review Committee. This Committee consists of the Cabinet or Chief Secretary and two other Secretaries of the Centre or State Government as the case may be. According to Rule 419-A(17), this Review Committee shall meet at least once every two months. The mandate of the Committee is to review whether the orders passed under sub-rule (1)[76] are in accordance with §5(2) of the Telegraph Act. Therefore, the Review Committee, after considering all relevant facts and circumstances, is meant to review whether a public emergency or a threat to public safety existed at the time of passing of the order. Further it must, after judicial application of mind, come to a conclusion about whether or not it was in the interest of public order, national security or sovereignty or protection of friendly relations with foreign States to pass the order of interception. A recent application under the Right to Information Act to the Ministry of Home Affairs has revealed that on an average 7500 to 9000 orders for interception are issued every month by the Central Government alone.[77] Therefore, if the Review Committee meets once every two months as it is statutorily mandated to do, then it would have to consider and dispose off between 15000 to 18000 orders of interception at every meeting. If, on the other hand, the Review Committee were to meet every day of the month it would have to dispose off between 290-345 orders. It is inconceivable that any three member body would be able to take into account all the relevant facts and circumstances surrounding 290 orders of interception in a day, let alone 18000. It is therefore clear that either the Review Committee undertakes its task in an extremely cursory manner or fails to even consider the vast majority of cases. If this is the case then despite the existence of Rule 419-A (16), India lacks any effective oversight of orders of surveillance. Hence, orders of interception passed under §5(2) are issued without any judicial scrutiny and even after their issuance are not subjected to any form of review. Therefore, a vast number of people whose communications are

---

[76] Rule 419-A (1), Indian Telegraph Rules, 1951 lists the authorities under Central and State Governments sanctioned to pass orders of interception.

[77] Rakesh Mittal, Director (Internal Security-I), Ministry of Home Affairs, Reply to Application of Ms. Shagun Belwal seeking information under the Right to Information Act, May 12, 2014 *available at* http://sflc.in/wp-content/uploads/2014/09/RTIreply_MHA_419A.pdf (Last visited on Aug. 18, 2016).

wrongfully intercepted are never even made aware of the serious infringement of their privacy by the State.

Despite the lack of any protection against the violation of its citizens' rights, India has been dangerously toeing the line that separates a democracy from a totalitarian surveillance State. In the last half a decade alone the Government has introduced tools that increase its surveillance capabilities manifold. Two of the most controversial tools alleged to have already been put into operation are the Central Monitoring System and the Network Traffic Analysis System (*hereinafter* "NETRA"). These projects have been tightly kept under wraps by the Government and most of the information available about them is speculative. Almost all the information available about these projects can be attributed to anonymous bureaucratic sources within the Government.[78] However, from whatever little information is available about these projects, they seem to fall within the ambit of the laws in operation governing surveillance.

NETRA has been developed by the Centre for Artificial Intelligence and Robotics (*hereinafter* "CAIR") laboratory at the Defence Research and Development Organisation (*hereinafter* "DRDO"). It appears to be designed to monitor packetised data and voice traffic over the internet using keyword searches.[79] As a tool that employs keyword searches to intercept communications, it will conduct dragnet surveillance. This form of surveillance will not discriminate between a malicious user and an innocent one, theoretically putting the entire internet user network under surveillance. NETRA, therefore, is a form of mass surveillance that will cause large scale breaches of privacy and unwarranted restriction on free speech and expression. Naturally, it begs the question of where exactly a tool designed for mass surveillance of a country's own citizens stands legally?

As a tool meant to be used strictly for surveillance over the internet, NETRA must necessarily function within the limits of §§69 and 69B of the Information Technology Act, 2000. §69 which is analogous to §5 of the Telegraph Act provides for interception of communication transmitted *via* a computer resource.[80] The procedure for intercepting communication transmitted over the internet has been laid down under the Information

---

[78] Press Trust of India, *India to deploy Internet spy system 'Netra'*, Live Mint, Jan. 06, 2014 *available at* http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html (Last visited on Aug. 18, 2016).

[79] Bhairav Acharya, NETRA: India's planned Orwellian surveillance system, Sep. 5, 2014 *available at* http://notacoda.net/2014/09/05/netra-indias-planned-orwellian-surveillance-system/ (Last visited on Aug. 18, 2016).

[80] Information Technology Act, 2000, §69.

Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (*hereinafter* "Decryption Rules"). Rule 9 of the Decryption Rules states that the direction of interception shall be with regard to any information that is sent to or from any person or class of persons or relating to any particular subject matter.[81] This is a significant departure from the interception that is allowed under the Telegraph and Post Office Acts. The Telegraph and Post Office Acts also allow the interception of communication relating to a person or a class of persons as well as any subject matter. However, owing to the physical nature of communication under the ambit of the Acts, only the communication of clearly identifiable individuals would be intercepted. Under the Decryption Rules, all persons over a computer network engaging in communication about a monitored subject matter would be brought under the ambit of surveillance. Therefore, the Decryption Rules authorise dragnet surveillance instead of targeted surveillance. The legality of this provision allowing bulk surveillance has not been called into question before Indian courts. However, as the matter stands, bulk surveillance is legally authorised in this country. A similar challenge that recently arose before the Investigatory Powers Tribunal in the UK does not inspire much optimism either. In Privacy International v. Govt. Communications Headquarters (*hereinafter* "GCHQ"), the legality of the GCHQ's involvement in the mass surveillance under the NSA's PRISM program and other similar activities was called into question.[82] The Tribunal considered the question of whether the practice of bulk data collection was permissible under the Regulation of Investigatory Powers Act, 2000 (*hereinafter* "RIPA"). Under the RIPA, §8(1) permits interception relating to only one person or one premise.[83] However, U/§ 8(4) non-targeted surveillance is also allowed so long as a warrant is obtained to that effect from the Secretary of State. While weighing in on the actions of GCHQ, the Tribunal said that it did not believe that §8(4) authorised bulk or mass surveillance and that such interception would be illegal.[84] It also rationalised GCHQ's position by stating that the espionage organisation's actions could not be called indiscriminate bulk surveillance, rather they should be considered "discriminate but vast"[85] surveillance. Here, the Tribunal while couching it

---

[81] Rule 9, Information Technology (Procedure ad safeguards for Interception, Monitoring and Decryption of Interception) Rules, 2009; also see Rule 3(4) of the Information Technology (Procedure and safeguards for Monitoring and Collecting Traffic Data or Information) rules, 2009.

[82] *Privacy International* v. *Govt. Communications Headquarters*, 2014 UKIPTrib 13_77-H.

[83] §8(1), Regulation of Investigatory Powers Act, 2000.

[84] *Privacy International* v. *Govt. Communications Headquarters*, 2014 UKIPTrib 13_77-H ¶71.

[85] *Privacy International* v. *Govt. Communications Headquarters*, 2014 UKIPTrib 13_77-H ¶72.

in slightly more politically correct terms has, in fact, indirectly given intelligence organisations a *carte blanche* to continue expanding their powers of interception. It is a legitimate fear that if the *vires* of the Decryption Rules are brought into question before the courts, a similar line of reasoning may be applied thus buttressing the perhaps already prevalent practice of dragnet surveillance.

As has been previously argued, communications can be intercepted on the mere belief that it is expedient in the interest of public order or national security. It has become apparent from the preceding discussion that the laws governing surveillance are not only archaic and ambiguous but also, in some cases, misguided. Over the last decade, the State instead of proactively modernising these legislations has been involved in creation of newer tools for restricting fundamental freedoms. In light of these developments, a serious revaluation of the existing laws has become imperative. The next part of the paper briefly discusses some practices that may be adopted to improve surveillance practices and minimise misuse.

VI. Suggested best practices for surveillance

Legal provisions governing surveillance and interception of communication in India are far from ideal. The very first infirmity that the legal setup suffers from is that the laws governing surveillance are outdated. The Information Technology Act, 2000 only regulates interception of communications transmitted over a computer network. The laws governing interception in other spheres are still archaic. Since the coming into force of the Telegraph Act there has been a sea change in technology that can remotely intercept communications over a telephone network. In 2012, the Department of Telecommunications issued a recall order for thousands of sophisticated phone interception devices that had been imported during the open general license regime.[86] These devices can remotely listen in and intercept phone conversations within a radius of two kilometres. It is believed that nearly 90% of these interceptors (codenamed FOX) had been purchased by private companies. However, despite the recall order, not one corporate entity declared that it was in possession of these devices.[87] Surveillance technologies

[86] Sanjay Singh, *Government hunts for elusive bug: DoT wants snooping and listening devices within private sector surrendered*, Daily Mail, Nov. 28, 2012 *available at* http://www.dailymail.co.uk/indiahome/indianews/article-2239422/Government-hunts-elusive-bug-DoT-wants-snooping-listening-devices-private-sector-surrendered.html (Last visited on Aug. 18, 2016).

[87] *Id.*

have moved far beyond the limitations that a hundred and thirty year old law could possibly impose on them. It is not just the government that possesses the capability of intercepting communications anymore. In spite of this, there have been no steps to draft specialised laws that protect citizens' privacy and insulate them from unauthorised surveillance either by the State or by private individuals. While almost all developed and developing countries have drafted progressive laws to enhance and better regulate their interception capabilities, India continues to be governed by an archaic law. This part exposits some aspects of the modern surveillance laws adopted globally, and discusses their viability in the Indian context.

One of the primary problems with Indian surveillance law is the executive authorisation model for intercepting communications. Both surveillance[88] and interception of one's communication[89] are a restriction on one's fundamental rights. They can therefore only be undertaken with due regard to procedure established by law. The right to privacy has been called too "broad and moralistic"[90] to be defined judicially. Any claim arising out of a violation of this right must be analysed on a case-to-case basis.[91] Therefore by necessary corollary, any restriction imposed on the right must also be determined with regards to the particular facts and circumstances of a case. An order of surveillance can impinge upon the right to privacy and impose a chilling effect on free speech. Every such order must be tested against the limits set under Article 19 of the Constitution. This determination can only be done adequately by a judicial officer and not by an executive authority. It is for this reason that almost all countries with specialised legislations for preventing unlawful surveillance have favoured a judicial sanction model over an executive authorisation one. In Australia, for instance, warrants for intercepting communications are granted by a judge or a nominated member of the Administrative Appeals Tribunal.[92] The Australian Telecommunications Interception and Access Act also clearly identifies which judges and nominated members are authorised to issue such warrants. In case of the nominated member, such member must have been enrolled as a legal practitioner of either a Supreme Court or a federal court for not less than five years.[93] It is only in case of an application for interception by the Australian Security Intelligence Organisation that a warrant is not required from a judge or a nominated member. But even so, a warrant must be obtained from the

---

88 *Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295 : (1964) 1 SCR 332.
89 *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568.
90 *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568.
91 *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568.
92 Telecommunications Interception and Access Act, 1979, §39.
93 Telecommunications Interception and Access Act, 1979, §6DB.

Attorney General after judicial application of mind.[94] In Brazil, wiretapping is regulated by the Federal Law No. 9,296. Under this law, authorisation for interception is granted on a judge's order for a period of 15 days at a time. Moreover, interception is only allowed for investigations into serious offences like drug smuggling, corruption, murder and kidnapping. The Canadian Criminal Code, 1985 which governs general rules of criminal procedure including search and seizure protocols, also favours the judicial sanction model. Under the Code, interception orders can only be issued by a provincial court judge or a judge of the superior court.[95] Similarly, in the United States, authorisation for interception can be granted by a District Court or a federal appeals court on application by a law enforcement officer duly signed by the Attorney General.[96] In France, the civilian law governing video surveillance and interception of communication also requires previous authorization from an investigating judge after consultation with the Public Prosecutor.[97] This reflects a clear lean in favour of letting the judiciary allow or disallow requests for interception of communications. The executive authorisation model, however, also finds some takers.

When it comes to authorising orders for interception, the United Kingdom, like India, goes against the grain. The UK has consistently followed an executive authorisation model for intercepting communications. Under the RIPA, UK grants authorisation for interception in the form of a warrant by the Secretary of State or in certain special cases by a senior officer.[98] It may be interesting to note here that most countries that have not drafted specialised legislations governing interception or have chosen to adopt the executive authorisation model are former colonies of the United Kingdom.[99] Telecommunications regulation in most of these countries is still governed by colonial laws. This may be attributed either to a lack of recognition of the right to privacy[100] or due to inadequate sensitisation of the citizens about State sanctioned surveillance.

---

[94] Telecommunications Interception and Access Act, 1979, §9.

[95] Canadian Criminal Code, 1885, §184.2.

[96] Electronic Communications Privacy Act, 1986 under Title III, Omnibus Crime Control and Safe Streets Act, §18.

[97] Loid'orientation et de programmation pour la performance de la sécuritéintérieure (LOPPSI 2), 2011, Article 36.

[98] Regulation of Investigatory Powers Act, 2000, §7.

[99] *See* generally, Privacy International's Country Reports on Iraq, Jordan, Malaysia, Sri Lanka and Bangladesh *available at* https://www.privacyinternational.org/resources/reports (Last visited on Aug. 18, 2016).

[100] *Privacy and Human Rights Report, 2006 for the Republic of Sri Lanka available at* http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html (The Sri Lankan Constitution does not explicitly recognize a right to personal privacy. The Country also lacks any specialized data protection framework) (Last visited on Aug. 18, 2016).

Exceptions however do exist. Of the countries that gained independence on a comparative time scale as India, only three have managed to draft specialised laws regulating interception. All three of these countries have opted for a judicial sanction model for intercepting communication. South Africa, having gained independence in 1931, drafted the Regulation of Interception of Communications and Provision of Communication-related Information Act in 2002. Under this law, a warrant for intercepting communications and installing surveillance devices is granted by a designated judge.[101] Such warrant is issued on satisfaction of the judge that the investigation relates to a serious offence or that the information gathering is vital to public health or safety, national security or compelling national economic interests.[102] Cyprus, that gained independence in 1960, drafted the Protection of Secrecy of Private Communications (Call Interception) Law in 1996. Under this Law, the Attorney General must file for a court order before using wiretaps.[103] The latest among the three countries to have modernised its surveillance laws is Pakistan. There, the power of law enforcement and intelligence agencies to intercept communications and undertake covert surveillance is governed by the Investigation for Fair Trial Act, 2013. The Act provides for a two-tiered supervisory model for authorising interception. Under §6 of the Act, every application for interception must be placed before the Federal Minister for Interior for his due consideration. It is only with the Minister's permission that the application can then be placed before a High Court Judge[104] for the issuance of a warrant.[105]

Modern tools and methods of conducting surveillance are complex and highly specialised. Moreover, the contours of privacy laws have not been well defined in India. Therefore, the determination of legitimate restrictions on the law of privacy is no simple task that can be left to the discretionary whims of a delegated administrative official. It is clear from the above discourse that in order to adequately regulate the practice of State sanctioned surveillance, it is necessary that the determination of a need for surveillance must be undertaken by the judiciary. The conditions listed under §5 of the Telegraph Act for interception can only be assessed by a judicial application of mind. No delegated administrative official is competent to make that determination. Therefore, warrants for ordering surveillance or intercepting

---

[101] Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, §16.

[102] *Id.* §19(4).

[103] Privacy International, Country Report on Cyprus (2012) *available a*t https://www.privacyinternational.org/resources/reports/cyprus#footnote1_1dd86bp (Last visited on Aug. 18, 2016).

[104] Investigation for Fair Trial Act, 2013, §9.

[105] Investigation for Fair Trial Act, 2013, §7.

communications must be issued by a Magistrate[106] or either a sitting or retired High Court Judge. In addition, laws governing surveillance must also be updated to keep up with vast leaps in the technology of intercepting communications. Some additional steps that can be taken to modernise the surveillance set up in India have been discussed below.

Along with a long overdue overhaul of the regulatory framework for interception, it is essential that the law must put in place adequate oversight mechanisms to prevent misuse of the law. Sub-rule 16 of Rule 419A provides for the establishment of a three-member Review Committee to review orders of interception. It also mandates that the committee meet at least once every two months. As has already been discussed, one meeting every two months is not nearly enough to thoroughly review all the orders passed under §5(2) of the Telegraph Act. The law should therefore mandate that the committee meet more frequently to be able to give due consideration to every order. Moreover, the constitution of the Review Committees has been limited to secretaries serving within the government. This has the effect of expecting the executive to conduct oversight on itself. Instead, it should be mandated that every Review Committee must have at least one judicial member who is independent of the government in power at the State or the Centre. In addition to the judicial member, the Review Committee should also include a member with technical expertise to deal with the increasingly complex issues of electronic surveillance such as encryption. Further, while the Rules provide some guidance with regards to duration for which intercepted data shall be retained,[107] they are completely silent with regards to inter-departmental sharing of such data. It is advisable that the legislature clarifies data sharing provisions under the Act. These protections may go a long way in helping reduce the misuse of surveillance powers by law enforcement and intelligence agencies.

VII. Conclusion

Surveillance causes a serious breach of one's privacy. Interception of communications restricts one's freedom of speech and expression by inducing a chilling effect. There have been proven cases of misuse of surveillance provisions in the past. With the invention of Orwellian tools for monitoring the lives of people, we have entered into a dangerous and uncharted territory.

---

[106] *See* Draft Privacy (Protection) Bill, 2013, §53 *available at* http://cis-india.org/internet-governance/blog/privacy-protection-bill-february-2014.pdf (Last visited on Aug. 18, 2016).

[107] Indian Telegraph Rules, 1951, Rule 419-A(18).

If the disclosures by former NSA employee Edward Snowden caution us of one thing then it is this: the State's machinery cannot always be relied on to act within the boundaries of law and display adequate respect for citizens' rights. It, then, falls onto all the stakeholders involved to ensure that the powers and functions of their correlative duty bearers are precisely defined. This paper has attempted to draw attention to systemic ambiguities and shortcomings in the existing legal regime. It has also attempted to highlight those aspects of the State's machinery that are vulnerable to misuse. To address these shortcomings, legislative and judicial authorities must not only look ahead but also draw lessons from the past. Creating a progressive and comprehensive legislation will only re-enact the failures from the past if the endemic problems in implementation are not resolved.

The absolute first step must be to address the ambiguities and shortcomings in the existing laws. For instance, oversight provisions, where they exist, must be strengthened, and where they don't exist, must be introduced. The Review Committee formed under Rule 419A has proven to be ineffective. Its powers, functions and constitution must be updated to actually help it discharge the duty it was established to discharge. The intelligence agencies that have been tasked with handling the information collection systems have not been created under any legislation and are therefore not subject to any parliamentary oversight. Attempts like the Intelligence Services (Powers and Regulation) Bill, 2011[108] have been shelved and not revisited since their introduction. Intelligence agencies that have been created through executive orders enjoy vast and unbridled powers that make them accountable to no one. They are putting the surveillance powers to the exact same kind of misuse[109] as it was subjected to in the past[110]. Before vesting the Indian law enforcement agencies with sensitive information that can be so readily misused, it is essential to ensure that a mechanism to check the use and misuse of that power exists.[111]

The second step must be the creation of progressive laws. The fountainhead of the solutions to all of these problems is a clear delineation of the right to privacy. A well-defined right to privacy will bring clarity to the focal point at which the State's power ends and a citizen's right begins. It is well

---

[108] The Intelligence Services (Powers and Regulation) Bill(2011) *available at* http://www.thehindu.com/multimedia/archive/00852/THE_INTELLIGENCE_SE_852812a.pdf (Last visited on Aug. 18, 2016).

[109] Saikat Dutta, *We, The Eavesdropped*, Outlook, May 3, 2010 *available at* http://www.outlookindia.com/article.aspx?265191 (Last visited on Aug. 18, 2016).

[110] Dutta, *supra* note 109.

[111] *See generally*, Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice, (2005).

past time and the legislature and the courts should revisit the question of specifically including a right to privacy within the fundamental rights.[112] Additionally, the legislature must undertake the herculean task of drafting a detailed and multidimensional legislation protecting physical, informational and locational privacy of individuals. A privacy protection legislation can do more than just delineate the scope of the right to privacy. It will help identify specific rights holders whose privacy is sought to be protected. It will assist in creating distinction between the privacy available to private individuals and public individuals. This may help resolve the long standing conflict between the right to privacy and freedom of speech and expression. Moreover, a legislation providing a right to privacy will also help identify the duty bearers who are obligated to not only deprive individuals of their privacy, but in certain cases even assist in the protection of the same.[113] Lastly, creating an explicit privacy legislation will also help dispel the erroneous notion that privacy is a western concept and finds no basis in Indian law. It will also help sensitise the citizenry about their right to privacy and inform them against potential violations of the same.

Over the last century, there have been very few attempts at redesigning the declining surveillance infrastructure in the country. Every single one of those attempts has ended with suggestions for improvement and modernisation of these laws. Each additional day that these draconian laws remain in operation, people's fundamental rights are threatened. However, we are now at a critical juncture. Never before has the Indian Government possessed the capability of restricting fundamental rights of the entire citizenry at once. With systems like CMS and NETRA possibly already in place, a legislative re-examination of these laws and institution of additional safeguards cannot come fast enough. Therefore, the one fact that becomes manifestly clear is that the data protection regime and surveillance powers of the State require a complete overhaul if even a vestige of privacy is sought to be protected.

---

[112] The National Commission to Review the Working of the Constitution in 2002 recommended that 'a right to respect for his private and family life, his home and his correspondence' be included as Article 21-B under the Fundamental Rights.

[113] *See generally*, Henry Shue, BASIC RIGHTS: SUBSISTENCE, AFFLUENCE AND US FOREIGN POLICY (1996).