SUPREMO AMICUS

VOLUME 24, MAY 2021 ISSN 2456-9704

SURVEILLANCE INDUCED CHILLING EFFECT ON SPEECH: CONSTITUTIONAL SAFEGUARDS IN INDIA AND USA

By Sejalsri Mukkavilli
From Alliance University, School of Law

ABSTRACT

Unfettered mass surveillance portends a declining democracy because it causes privacy harms which eventually plummet into free speech concerns and erodes the structural roles of checks and balances owing to lack of transparency which prevents the judiciary from exercising its check of judicial review on the ever expanding executive branch. While the violation of privacy may disrupt valuable activity, it also causes a chilling effect. Chilling effect refers to "a practice of self-censorship that citizens engage in to avoid being penalized for illegal speech." Both the USA and India, have emerged as democracies that qualify for comparison. Considering how the American Bill of Rights became the harbinger of the fundamental rights enshrined in the Indian Constitution, Indian free speech and privacy jurisprudence draws extensively from the American jurisprudence. Both democracies exhibit large military spending, emphasizing the State's massive interest in 'national security' and surveillance as means to achieve it in both countries. This paper aims to comparatively analyse the free speech safeguards guaranteed in both of these jurisdictions vis-a-vis surveillance. The first part of the paper explains the right to privacy of speech, essentially delineating the interrelationship between privacy and free speech. The second part discusses the evolution of privacy related claims vis-a-vis surveillance in India and the same is comparatively analysed with USA's own jurisprudence. The third part explains how surveillance operates under existing laws in India. The last part of the paper explores the inadequacies in the existing legal situation, including the incoming data protection bill and the need to amend it. The objective of the paper is to analyse how effective are constitutional free speech safeguards against surveillance laws in both the jurisdictions.

Keywords: Free speech, privacy, surveillance, India, USA, comparative constitutional law.

1. INTRODUCTION

Freedom of speech and expression inheres central importance in contemporary political thought and practice. The extent of a democracy directly correlates to the existence of, *at least*, a constitutional guarantee of freedom of speech and expression as an individual right which is enforceable against the government in a court of law. Extrapolating Habermas' Theory of Legitimacy,[1] Robert Post notes that

[1]Gautam Bhatia, 'Understanding Free Speech' in *Offend, Shock or Disturb: Free Speech Under the Indian Constitution*, (Oxford University Press 2018) p. 21: Habermas observes that a "law which mandates a particular course of action is valid and binding upon its subjects only if it is agreed upon by all possibly affected persons participating in a rational discourse. A rational discourse is …a discussion in which participants genuinely want to convince one another...by the force of the better argument. In order to achieve this, Habermas places a series of structural constraints upon the discourse...*inclusion* and *equality*. The Inclusion Principle stipulates that every subject with the competence to speak and act is allowed to participate. The Equality Principle requires that no speaker may be prevented, by interna; or

democratic legitimacy can be accorded through communications that occur in the public. And that, 'speech' refers to all forms of communication that are socially indispensable for facilitating proper means of participating in formulating public opinion. Individuals participating in the public discourse ought to be included by enabling access to public spheres and their voices should be accorded equal protection as that of others.[2] According to Post, the meaning of 'public sphere' would be a normative assessment- a proposition that now concocts more controversies than before. The upshot is that surveillance occurs in the private spheres, yet its complications spill into the public lives of a State's citizenry.

The Centre for International Governance Innovation explains state surveillance as "Such activities including surveillance, understood here as any personal data acquisition and analysis for management, influence or entitlement."[3] The CIGI also elaborates that, "Externally, surveillance relates to geopolitical and military purposes or commercial advantage. Internally, surveillance might be pursued for the pacification and administration of the population. This includes the collection and use of data for everything from electoral rolls to health care and welfare provision."[4]

Unfettered mass surveillance portends a declining democracy because it causes privacy harms which eventually plummet into free speech concerns and erodes the structural roles of checks and balances owing to lack of transparency which prevents the judiciary from exercising its check of judicial review on the ever expanding executive branch.

Privacy violations cause not only dignitary harm; it can also cause the enhancement of the risk that a harm will occur- increasingly accessible information about a person can expose such a person to risks of fraud or identity theft; the imbalance of power between the individual and governments and corporations holding our information, can make us anxious and hyper aware about our actions and speech, and cause people to refrain from exercising their right to critical speech of mainstream values and attending protests. While the violation of privacy may disrupt valuable activity, it also causes a chilling effect.[5] Chilling effect refers to "a practice of self-censorship that citizens engage in to avoid being penalized for illegal speech."[6]

Surveillance laws are always weighed against balancing individual and societal interests couched in words such as national security. However, this a misrecognition of scale, privacy and it's chilling effect on free speech harbour societal interests. Privacy and free speech can no longer be embedded in the traditional logic of 'individual rights'. Sociologist Barrington Moore has maintained that privacy protection is a socially created need. Since, people engage in many activities that indispensably yoke us to other individuals, institutions and

external coercion, from exercising his rights as above."

[2] *Ibid.*

[3] David Lyons, 'State and Surveillance' (*CIGI*, 1 May 2009) <http://www.nakedlaw.com/2009/05/index.html> accessed 19 November 2009.

[4] *Ibid.*

[5] Chinmayi Aru, 'PAPER-THIN SAFEGUARDS AND MASS SURVEILLANCE IN INDIA' 26(2), (2014) National Law School of India Review, 105-114 <https://www.jstor.org/stable/4428363> accessed 12 March 2021.

[6] *Ibid,* (n 3).

governments, private actions can have adverse impacts on others. The need to protect one's privacy stems from frictions and conflicts that are embedded in the social fabric and it is here, where privacy emerges as a relief from exposing oneself to such friction and conflict. However, privacy is only a protection from a cluster of activities that impinge on other people in related ways and is not an absolute protection from all forms of social friction.[7] Understanding privacy and free speech as societal concerns commandeer governmental focus on transparent and accountable mechanisms. India's repressive enforcement of its infamous terrorism legislation, the sedition law, and even its brazenly speech restricting internet regulation rules, and its status as the "global capital of internet shutdowns" has characterized it as an electoral autocrcacy.[8]
Both the USA and India, have emerged as democracies that qualify for comparison. Considering how the American Bill of Rights became the harbinger of the fundamental rights enshrined in the Indian Constitution, Indian free speech and privacy jurisprudence draws extensively from the American jurisprudence. Both democracies exhibit large military spending, emphasizing the State's massive interest in 'national security' and surveillance as means to achieve it in both countries. This paper aims to comparatively analyse the right to privacy of free speech safeguards guaranteed in both of these jurisdictions against state surveillance.
India's declining status in democractic freedoms is alarming. With the government of India introducing laws that purvey to some form of surveillance, this has caused a chilling effect in the Indian citizenry constructively suppressing socially beneficial speech, surveillance laws are becoming increasingly pertinent in India.

The first part of the paper explains the right to privacy of speech, essentially delineating the interrelationship between privacy and free speech. The second part discusses the evolution of privacy related claims vis-a-vis surveillance in India and the same is comparatively analysed with USA's own jurisprudence. The third part explains how surveillance operates under existing laws in India. The last part of the paper explores the inadequacies in the existing legal situation, including the incoming data protection bill and the need to amend it. The objective of the paper is to analyse how effective are constitutional free speech safeguards against surveillance laws in both the jurisdictions.

2. THE RIGHT TO PRIVACY OF SPEECH

The word privacy suffers from its polysemic quality, constantly varying on the bedrock of context. This has made privacy very difficult to discern. Everyone, almost instinctively, can identify a privacy harm, yet scholarship on privacy has been in a monosemic and unvarying fashion. Solove's *A Taxonomy of Privacy*[9] is a remarkable contribution in attempting to articulate so comprehensively the multifarious facets of privacy harms. Since, the scope of this paper is limited to

[7] Barrington Moore, Jr., 'Privacy: Studies in Social and Cultural History', 73 (1984).

[8] Sweden's V-Dem (Varieties of Democracy) Institute, in its report titled, "Autocratization Goes Viral", downgraded India from the world's largest democracy to an electoral autocracy. It cited "restrictions on multiple facets of democracy".

[9] Daniel J Solove, 'A Taxonomy of Privacy', 154 (3) (2006) University of Pennsylvania Law Review, 477-560 <A Taxonomy of Privacy by Daniel J. Solove :: SSRN> accessed 18 April 2021.

addressing surveillance induced privacy harms of free speech, the author draws from Solove's aforesaid work to exclusively articulate the conceptual soldering of privacy related free speech harms (explained in the following sections). However, the broad scheme of Solove's Taxonomy has been produced hereunder, to provide a concise and crucial understanding of privacy harms. Solove maintains that there are four basic groups of privacy harms[10]:

(1) INFORMATION COLLECTION- Involves the probing of information from the data subject by the data holders.

- *Surveillance*- it consists of a persistent watching, listening to or recording of the data subject's activities.
- *Interrogation*- consists of various forms of questioning or probing for information.

(2) INFORMATION PROCESSING- Involves the storing or maintaining, manipulating or using of the data subject's information.

- *Aggregation*- is the collation of the data subject's myriad and dispersed information.
- *Identification*- is designating information so gathered and aggregated to a particular individual.
- *Insecurity*- is the data holder's failure to protect stored information from data leaks and unauthorized access.
- *Secondary Use*- occurs when information provided for an authorized purpose is used for a different purpose without the data subject's consent.
- *Exclusion*- when the data subject is prevented from learning about the way in which their data is being handled and used.

(3) INFORMATION DISSEMINATION- Involves the spreading or transfer of personal data or the threat to do so.

- *Breach of Confidentiality*- occurs when the data holder fails to maintain the promise of securing the data subject's confidentiality.
- *Disclosure*- is the divulgence of truthful information about the data subject having a propensity to impact other people's judgment about them.
- *Exposure*- is revealing another's nudity, grief and bodily functions.
- *Increased Accessibility*- increasing the scale of access to the data subject's information.
- *Blackmail*- the threat to disclose personal information.
- *Appropriation*- the data subject's information is used to serve particular aims and interests of another.
- *Distortion*- the data subject's information is distorted through false and misleading dissemination.

(4) INVASION

- *Intrusion*- inroad into a person's private affairs causing the disruption of the person's solitude and tranquility.
- *Decisional Interference*- when the data subject's decision making about their own private affairs becomes impacted by the government's interference into their private affairs.

2.1. Chilling Effect:

Privacy related free speech harms can be best explained through the concept of chilling effect. Chilling effect occurs when citizens indulge in a practice of self-censorship to protect themselves from being penalized for illegal speech and expression. However, this self censorship is of such a scale that, the fear of punishment will compel people to grow

[10] *Ibid*: "I have arranged these groups around a model that begins with the data subject– the individual whose life is most directly affected by the activities classified in the taxonomy. From that individual, various entities (other people, businesses, and the government) collect information."

anxiously conscious of the distinction between legal and illegal speech, so much so that, they will refrain from exercising even their constitutionally protected speech, thereby serving a silencing function or the *chilling effect* of critical speech which is important for effective democratic politics and public accountability. The chilling effect usually occurs when laws suffer from overbreadth- the ambiguities of the words used therein, causes people to self censor so that they remain unambiguously law abiding.[11]

The word "chilling effect" was extensively associated with the American defamation law, to express the common law coherence of placing a high burden of proof on the defendant to prove material truthfulness to the impugned defamatory remarks, coupled with the remedy of paying exemplary damages which made it an increasingly deployed tool by governments and corporations to silence critical speech. The chilling effect of the defamation law was well recognized and acknowledged in America's landmark judgment- *New York Times v Sullivan*.[12] The New York Times had been doing extensive coverage on the civil rights movement. Alabama state officials brought a defamatory claim of three million dollars against New York Times for its reportage which contained some minor factual inaccuracies. The amount of compensation claimed would have driven the New York Times to bankruptcy and would have disabled the news coverage on the civil rights movement. The court ruled unanimously in favour of the newspaper and held that, in libel cases, falsehood in statements made are punishable only if it was known to the publisher. The judgment observes thus, '...the chilling effect that Alabama's libel laws have on the First Amendment.'

The concept of 'chilling effect' is recognized even in India's free speech jurisprudence. It has also been used in the context of privacy of sexual autonomy and expression. For instance, in *Navtej Singh*[13], it was held that Section 377 IPC amounts to unreasonable restriction as it makes carnal intercourse between consenting adults within their homes a criminal offence which is manifestly not only overbroad and vague but also has a chilling effect on an individual's freedom of choice.[14] In *K S Puttaswamy*[15], chilling effect has been used to overrule the 'de minimis'[16] hypothesis that the Court in *Koushal*[17] had presented. The Court held that the de minimis hypothesis is misplaced since the infringement of fundamental rights does not become tolerable only because a negligible size of population had been adversely impacted. The reason why such acts of hostile discrimination are constitutionally impermissible is because of the chilling effect which they have on the exercise of the fundamental right in the first place. The chilling effect on the exercise of the right

[11] Gautam Bhatia, 'Common Concepts' in *Offend, Shock or Disturb: Free Speech Under the Indian Constitution*, (Oxford University Press 2018), p. 32.
[12] *New York Times v Sullivan*, 376 US 254 (1964).
[13] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.
[14] *Ibid*, p. 142, para 261.
[15] *K S Puttaswamy (Privacy- 9J) v Union of India*, (2017) 10 SCC 1.
[16] Koushal based its reasoning (denying the right to life, privacy and free expression to LGBT folks) on the basis that only a minuscule population of the LGBT community had been prosecuted thus far and that no profound dignitary harms had been caused by section 377 IPC.
[17] *Suresh Kumar Koushal* v. *Naz Foundation*, (2014) 1 SCC 1.

poses a grave danger to the unhindered fulfilment of one's sexual orientation, as an element of privacy and dignity. The chilling effect is due to the danger of a human being subjected to social opprobrium or disapproval, as reflected in the punishment of crime. In *Shreya Sighal*[18], in striking down section 66A of the IT Act as unconstitutional, the court held that the words in the section is cast in such wide terms that virtually any opinion on any subject could be made punishable under it, and that restrictions on free speech should be couched in the narrowest possible terms so as to fulfill the test of reasonable restrictions under Article 19(1)(a) and (2), lest it will have a chilling effect on free speech.

2.2. <u>Surveillance Induced Chill on Speech:</u>

Solove writes, in some contexts, the direct awareness of surveillance can create feelings of anxiety and discomfort to the extent that a person may alter their behaviour which can amount to "self-censorship and inhibition." Surveillance is endorsed by some as means of social control. It is said to have a deterrent effect of sorts, when people are aware they are being watched or listened to, they may refrain from doing anything illegal for fear of being caught. However, too much social control can be stifling, impinging the "freedom, creativity and self-development" of the individual. Scholars have noted the effects of surveillance in mainstreaming people's own individual oddities and thoughts by constraining "acceptable spectrum of behaviour and beliefs" and thereby serving a chill on the expression of people's essential individuality that may seem odd to others and expose them to suspicion from law enforcement agencies.[19]

What kind of harm can covert surveillance cause to its subjects? To answer this, Solove relies on Jeremy Bentham's Panopticon Prison Model. Bentham argued for a prison with a tower at the centre and a periphery building composed of cells from which every inmate could be observed but the inmates could not see the guards from their cells. The cells would all have windows that would enable surveillance by prison guards. The inmate would have no option but to conform with the prison rules since they could be watched at any given time and moment by the guards. Solove argues that when people are generally aware of the possibility of surveillance but are not specifically aware of the medium and the particular time and moment at which they are being watched, the resulting chilling effect can be far more profound.

Then what kind of harm can covert surveillance cause if its subjects are completely unaware of the possibility of being watched? Since, the complete lack of awareness will rule out feelings of anxiety and discomfort or chilling effect in its subjects, covert surveillance can still cause harms- such as a complete profile of its subjects can be made by seizing information and such information may be used for more than just 'investigative' purposes, it may be used for recording behavior and for virtually anything beyond the scope for which it was initially gathered. This information so ensnared can be used to watch the subject and if the subject is caught doing something illegal, the same information can be used for exposure, blackmail, distortion and appropriation.[20] Thus, the impacts of surveillance can go beyond causing a chilling

[18] *Shreya Singhal v Union of India,* (2015) 5 SCC 1.

[19] *Ibid,* (n. 10) See page 494.

[20] *Ibid,* (n. 10): A prime example is the FBI's extensive wiretapping of Martin Luther King, Jr., widely

effect on speech, however, the freedom of speech and expression is surely impacted through surveillance.

In *KS Puttaswamy*,[21] India's one-stop jurisprudence on the right to privacy, the court has regarded the right to privacy as the core intersticed within all other fundamental rights in part III. Interpreting the right to privacy as an enabling and facilitative right of individual autonomy for the enjoyment and exercise of all liberties guaranteed under Part III, the court more specifically, pointed to the interrelationship between privacy and the expressive freedoms under Article 19. This deduction stemmed from the *Maneka Gandhi*[22] doctrine which held out the interrelationship between the fundamental rights in Part III. In *KS Puttaswamy*, the court observed that the essence of the various expressive freedoms guaranteed is springed on a corresponding guarantee of cognitive freedom. This cognitive freedom creates a condition whereby it is impossible to selectively seclude the exercise of one freedom from another. In other words, it is not possible to detach the basic freedom to do an activity in seclusion, from the freedom to do the activity itself. Thus, the privacy of an individual recognizes an inviolable right to determine how the freedoms shall be exercised. Surveillance, by springing up feelings of discomfort and potent breaches of information privacy which spill into privacy harms of dissemination and invasion, hinders the overall freedom of an individual to exercise their expressive freedoms in seclusion and repose from social censure.

2. THE CONSTITUTIONAL LAW DEFINING THE RIGHT TO PRIVACY OF FREE SPEECH

3..1. The Evolution of India's Surveillance Related Right to Privacy Jurisprudence:

In *Kharak Singh*[23], the court struck down Regulation 236(b) of the UP Police Act which allowed the police to run nocturnal domiciliary visits on the ground that the regulation invaded the sanctity of the home and was a violation of ordered liberty and "personal liberty" protected under Article 21. Though the reasoning of the Court does not use the expression "privacy", it alludes to the decision of the US Supreme Court in *Wolf* v. *Colorado*[24] which deals with privacy. Contrary to this tacit acknowledgement of a right to privacy, the court upheld the other impugned regulations maintaining that the Constitution did not recognize a protected right to privacy. However, subsequent benches have attempted to rely on the first part of the decision in *Kharak Singh*.

In *Malkani*[25], the court upheld the validity of Section 25 of the Indian Telegraph Act, 1885. The impugned section was challenged on the ground that it violated the privacy of the appellant's conversation under Article 21. This court followed the same line of reasoning as it had in *Kharak Singh* while rejecting a privacy-based challenge under Article 21. Article 21 contemplates

believed to have been initiated in order to expose King's alleged communist ties. Though the surveillance failed to turn up any evidence of such ties, it did reveal King's extramarital affairs. The FBI then attempted to blackmail King.

[21] *Ibid*, (n. 16).

[22] *Maneka Gandhi v Union of India*, (1978) 1 SCC 248.

[23] *Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295.

[24] *Wolf* v. *Colorado*, 1949 SCC OnLine US SC 102.

[25] *R.M. Malkani* v. *State of Maharashtra*, (1973) 1 SCC 471.

procedure established by law with regard to deprivation of life or personal liberty. The court ruled that the telephone tapping of an innocent citizen will be protected against wrongful interference by wiretapping, while telephone tapping directed at a guilty person would be saved by "procedure established by law".

In *Gobind*[26], a Bench of three Judges of this Court considered a challenge to the validity of Regulations 855 and 856 of State Police Regulations under which a history sheet was opened against the petitioner who had been placed under surveillance. The court proceeded on an assumption of a guaranteed right to privacy but did not enter a specific finding on the existence of a right to privacy and explained what the content and extent of the right would have entailed. The court relied on US cases like *Griswold* v. *Connecticut*[27] and *Roe* v. *Wade*[28] which recognized the right to privacy and also cited Brandeis J. dissent in *Olmstead* v. *United States*[29]. *Gobind* observed that the right to privacy would be intrinsic to ordered liberty and would cover intimate matters such as family, marriage and procreation, while also holding that such a right would not be absolute and the right could be curtailed by the state subject to two limitations on the state's power to do so: (i) there must be a compelling state interest and (ii) a narrow tailoring of the law to meet the compelling state interest.

In *Malak Singh*[30], the court dealt with the provisions of Rule 23 of the Punjab Police Rules under which a surveillance register was to be maintained among other persons, of all convicts of a particular description and persons who were reasonably believed to be habitual offenders whether or not they were convicted. The Rules provided for modalities of surveillance. The Court in *Malak Singh* did not consider it unlawful for the police to conduct surveillance so long as it was for the purpose of preventing crime and was confined to the limits prescribed by Rule 23 which, while authorising a close watch on the movement of a person under surveillance, contained a condition that this should be without any illegal interference. Surveillance of persons who do not fall within the categories mentioned in Rule 23 or for reasons unconnected with the prevention of crime, or excessive surveillance falling beyond the limits prescribed by the rules, will entitle a citizen to the court's protection which the court will not hesitate to give. Without specifically holding that privacy is a protected constitutional value under Article 19 or Article 21, the judgment of this Court indicates that serious encroachments on privacy impinge upon personal liberty and the freedom of movement.

In *Rajagopal*[31], a writ was sought under Article 32 for restraining the State and Prison Authorities from interfering with the publication of an autobiography of a death row convict prisoner in a magazine. The

[26] *Gobind* v. *State of M.P.*, (1975) 2 SCC 148.
[27] *Griswold* v. *Connecticut*, 1965 SCC OnLine US SC 124: In which a conviction under a statute on a charge of giving information and advice to married persons on contraceptive methods was held to be invalid.
[28] *Roe* v. *Wade*, 1973 SCC OnLine US SC 20: In which the Court upheld the right of a married woman to terminate her pregnancy as a part of the right of personal privacy.
[29] *Olmstead* v. *United States*, 1928 SCC OnLine US SC 131.
[30] *Malak Singh* v. *State of P&H*, (1981) 1 SCC 420.
[31] *R. Rajagopal* v. *State of T.N.*, (1994) 6 SCC 632.

Prison Authorities maintained that any publication based on a convict went against the Prison Rules and also denied that the autobiography had not been authored by the convict himself. The court considered a question concerning a balance between the prisoner's right to privacy against an unauthorized publication and a citizen's right to speech and expression in writing about the life of another citizen. Relying on the decisions in *Kharak Singh* and *Gobind*, Jeevan Reddy, J. acknowledged that the right to privacy was implicit in the right to life and personal liberty under Article 21. The court reasoned that, although Kharak Singh and Gobind referred to the right of privacy, the decision primarily relied on the content of "life and personal liberty" in Article 21.

In *PUCL*[32], the court dealt with telephone tapping. The petitioner challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885 on the grounds that the section was infringement of the right to privacy under Articles 19(1) and 21, and urged in the alternative for adopting procedural safeguards to curb arbitrary acts of telephone tapping. *PUCL* harmoniously construes the majority opinion of the *Kharak Singh* court which struck down Regulation 236(b) empowering the police to conduct nocturnal domiciliary visits, and the minority opinion of Subba Rao, J. as having gone even further by invalidating the entire Regulation 236 in recognizing an intrinsic right to privacy in Article 21. The court therefore ruled that telephone conversations which are often of private and intimate nature are protected under the right to privacy. Telephone tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law. The Court also held that telephone tapping infringes the guarantee of free speech and expression under Article 19(1)(*a*) unless authorised by Article 19(2).[33] The decision in the *State of Maharashtra* v. *Bharat Shanti Lal Shah*[34] dealt with the constitutional validity of Sections 13 to 16 of the Maharashtra Control of Organised Crime Act which inter alia contains provisions for intercepting telephone and wireless communications. The court upheld these provisions by relying on Section 14 which provided for safeguards entailing that surveillance could be authorized only upon the details of the organized crime that is about to be or is being committed, the nature and location of the facilities from which the communication is to be intercepted, the nature of the communication and the identity of the person, if it is known. The provision expressed surveillance as the last resort only where other modes of intelligence gathering failed, or if other modes would be dangerous so as to disclose the identities of the people involved in the operation. The duration of the surveillance is restricted in time and the provision requires minimal interception.

However, all the above case laws which dealt with state surveillance and the right to

[32] *PUCL* v. *Union of India*, (1997) 1 SCC 301.

[33] In the absence of rules providing for the precautions to be adopted for preventing improper interception and/or disclosure of messages, the fundamental rights under Articles 19(1)(*a*) and 21 could not be safeguarded. But the Court was not inclined to require prior judicial scrutiny before intercepting telephone conversations. The Court ruled that it would be necessary to lay down procedural safeguards for the protection of the right to privacy of a person until Parliament intervened by framing rules under Section 7 of the Telegraph Act. The Court accordingly framed guidelines to be adopted in all cases envisaging telephone tapping.

[34] *State of Maharashtra* v. *Bharat Shanti Lal Shah*, (2008) 13 SCC 5.

privacy and free speech and expression, resulted in a confusion which stemmed from *Kharak Singh* having delivered a judgment which confronted conflicting observations, and all the subsequent judgments which had adverted to *Kharak Singh*- were of smaller benches. The confusion was resolved in the *KS Puttaswamy (9- judges)* case in 2017 which overruled *Kharak Singh* decision to the extent that it had held that there is no right to privacy guaranteed under our Constitution.

3.2. Tests Defining the Restrictions on the Right to Privacy of Free Speech:

In *KS Puttaswamy*, the court has established a cogent link between Article 21 (broadly) in that the right to privacy, and Article 19(1) in that of expressive freedoms- of which the freedom of speech and expression is a part.[35] The judgment also discusses all the tests for determining the limits on the State in restriction privacy.

The Interrelationship Between the Fundamental Rights Test:

KS Puttaswamy holds that, if a law encroaches upon privacy, it will have to withstand the touchstone of permissible restrictions on fundamental rights to which privacy in that situation relates to. The inevitable and the first task of the court would be to test the invasion of privacy under the parameters of Article 21, since the right to privacy directly flows from Article 21. In this regard, the court would have to satisfy itself to the following requirements:

(i) Legality, which postulates the existence of a law;

(ii) Need, defined in terms of legitimate state aim; and

(iii) Proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them.

The state's interference with the right to privacy must be tested against whichever one or more Part III guarantees whose enjoyment is curtailed. Thus, if a privacy claim specifically flows from one of the expressly enumerated provisions under Article 19(1)(a), then the standard of review would be as expressly provided under Article 19(2). The restrictions upon Article 19(1)(a) must conform to the eight specific categories of Article 19(2), each of which has a defined meaning.[36] The test for the restrictions in Articles 19(2) to (6) is that of the 'test of reasonable restrictions'[37] and the 'effect and subject matter test'[38]. For instance, *Shreya Singhal* is a notable jurisprudence on free speech restrictions in India. The case dealt with the constitutional validity of section 66A of the IT Act which made punishable the

[35] This has been explained in the previous Section 2.2.

[36] *Shreya Singhal*, para 21.

[37] Restrictions can be imposed only by or under authority of law, no restriction can be imposed on by executive action alone, without there being a law to back it up. Each restriction must be reasonable. In *State of Madras v VG Row*, the court said that the word 'reasonableness' cannot be defined and has to be discerned from a case by case approach. Reasonableness may also be understood in the context of Article 14 contemplating a right against arbitrariness. There must be a proximate nexus between the restriction imposed and the object sought to be achieved. Also, reasonableness must be tested on both substantive and procedural points. The restriction must be strictly within the confines of the enumerated purposes mentioned in clauses (2) to (6).

[38] Although the subject matter of the impugned law may purport to be within 'reasonable restrictions', if the direct or indirect effect of the law is such that it is excessive or arbitrary, then it will be struck down.

sending of an "any grossly offensive…" information through computer resources. Four arguments were presented in the judgment which struck down the section: first, the terms 'grossly offensive', 'menacing', 'annoying', 'inconvenient' which appeared in the section, failed to observe the proximity test as a public order restriction; second, section 66A is vague; third, section 66A is overbroad; fourth, the vagueness and overbreadth is likely to result in causing a chill on the freedom of speech. It was also observed by the Law Commission in its 38th Report, that surveillance should be undertaken only if it was necessary under one of the grounds listed in Article 19(2).72

Moreover, in drawing the interrelationship between Part III rights also noted that the test against arbitrariness which is manifest in Article 14 can be extended to the right to privacy. Since, the right of equality is a right against state arbitrariness which prevents discrimination between individuals, the destruction by the state of an individual's sanctified space- whether body or mind is an arbitrary act which seeks protection under Article 14.

The Compelling State Interest Test:

Chelameswar, J. in *Gobind* resorted to the 'compelling state interest' standard in addition to the just, fairness and reasonable enquiry under Article 21. The term comes from American jurisprudence however, remained undefined. The American jurisprudence had evolved two necessary conditions to qualify a restriction on privacy: a compelling state interest and a narrow tailoring of the law i.e., the law must be narrowly framed to achieve the object. Thus, for the purpose of free speech, it must be shown that the state had a compelling interest. The state's compelling interest is covered within the restriction in Article 19(2) under the eight specified heads, each of which have their own defined parameters.

The Choice and Specification Test:

S A Bobde, J. in *Puttaswamy*, formulated the choice and specification test. The honorable Justice noted that, to exercise one's right to privacy is to choose and specify on two levels- it is to choose which of the various liberties available to her would she like to perform and which of them not to perform, and to specify whom to include or/and exclude in engaging with or witness her performing them.[39] In the words of the honourable justice, "*To check for the existence of an actionable claim against an infringement of the right to privacy, all that needs to be considered is if such an intent to choose and specify exists, whether directly...in the right bearer's actions, or otherwise. Such a formulation would exclude three red herrings- firstly, it would not admit arguments that privacy is limited to property or places...Secondly, this formulation would not reduce privacy to solitude...Thirdly, neither would such a formulation require to hold that private information is inaccessible to all others.*"[40] On a similar tangent, a privacy claim asserting the freedom of speech must show the rights bearer intended to choose what to say and express, and specify to exclude the state from bearing audience to what she said or expressed. The intention to choose and specify may be determined from another test evolved under

[39] Contains the positive and negative autonomy to choose and specify.

[40] *Puttaswamy*, para 424 and 425.

American jurisprudence- the test of reasonable expectation of privacy.[41]

3.3. A Comparative Analysis of Surveillance Related Right to Privacy of Speech with the USA:

Although the American constitution contains no express right to privacy, the Supreme Court has been able to locate the right from several provisions of the Bill of Rights- a position which is the same in India. Several provisions of the Bill of Rights were adopted to protect individuals from unreasonable invasions of privacy[42]:

(1) The Third Amendment explicitly protects the privacy of the home in peacetime from soldiers seeking quarters.
(2) The Fourth Amendment protects individuals from unreasonable searches and seizures where they have a "reasonable expectation of privacy".
(3) The Fifth Amendment prohibits compulsory self-incrimination, thus protecting the privacy of an accused individual's thoughts.
(4) The First Amendment ensures freedom of conscience in both political and religious matters, again recognizing the autonomy of the individual. The implicit guarantee of the freedom of association has been read into the right to choose one's friends, one's spouse, one's business partners, and so on. The court in *Griswold v. Connecticut*[43], has held that the constitution protects such relationships and decisions in the private realm from government intrusions.
(5) In *Griswold*, the court referred to the Ninth Amendment, which guarantees rights "retained by the people" even though they are not enumerated in the Constitution.

All the unenumerated constitutional rights[44] which the courts have come to recognize have now been maintained as elements of "liberty" protected by the Due Process Clauses of the Fifth and Fourteenth Amendments.

Insofar as surveillance related privacy is concerned, a more proximate constitutional protection to the American citizens is the Fourth Amendment which recognizes a right of personal privacy entitling the American people to protection against arbitrary intrusions by law enforcement officers. The historical antecedents of the Fourth Amendment was a criticism of the excessive powers of the police and customs officials to conduct "general searches" under Writs of Assistance.[45] On the other hand, the framers of the Indian Constitution opted to decline the recognition of an express right of "secrecy of correspondence and protection from unreasonable search and seizures". Objections were raised which expressed hindrances over the complication of administering justice on grounds such as that, the protection would affect the prosecution especially in cases of conspiracy or abetment; that this would seriously affect the powers of investigation of the police; that it would

[41] This is discussed below in section 3.3.
[42] Otis H Stephens, Jr., John M. Scheb, *American Constitutional Law: Civil Rights and Liberties* (Vol II, 4th edn., Thomson Wadsworth 2008).
[43] *Griswold* v. *Connecticut*, 1965 SCC OnLine US SC 124.
[44] The right to marry, to choose one's spouse, to select an occupation, to travel freely within the country, and to enter into contracts are all examples of long-standing rights retained by the people although they are not explicitly provided for in the Constitution.
[45] *Ibid*, (n. 43): Warrants that did not specify the persons to be searched or arrested, the premises to be searched, the number of persons or items to be seized, the nature of the items to be seized, or even the reason for the warrant.

abrogate some of the provisions of the Code of Criminal Procedure; it would constitute a serious impediment in prosecutions; the protection against unreasonable searches and seizures was deleted on the ground that there were provisions in the Code of Criminal Procedure, 1898 covering the area. However, the Court in *KS Puttaswamy* refused to take an originalist interpretation and held that the a variety of rights have been read into and subsumed within the existing liberties in Part III- such a stance has been possible because of precedents such as *RC Cooper*[46] and in the post *Maneka* age. It is now a settled principle of law that the liberties in Part III are not ensnared in tight watershed compartments, and that the liberties are not mutually exclusive but that they are overlapping and thus, a liberty infringed under Article 19 is bound to have infringed Article 21. Therefore, a right to privacy can be discerned in both the Articles.

In the US, the right to privacy had been recognized as early as the 1886 in *Boyd v US*[47] which recognized the modern concept of informational privacy whereby the court held that a compulsory production of a person's private papers to be used as evidence against him in a judicial proceeding is an unreasonable search and seizure within the meaning of the Fourth Amendment. In *Meyer v Nebraska*[48] and *Pierce* v. *Society of Sisters*[49] the Court read the Fourteenth Amendment's liberty to prohibit States from making laws interfering with the private decisions of parents and educators to shape the education of their children.

In *Olmstead* v. *United States*[50], the question before the Court was whether the use of evidence of private telephone conversations, intercepted by means of wiretapping amounted to a violation of the Fourth and Fifth Amendments. In a 5 : 4 decision, it was held that there was no violation of the Fourth and Fifth Amendments and reasoned that the amendment itself shows that the search is to be of material things- the person, the house, his papers, or his effects and that the amendment does not forbid wiretapping since there was no searching nor seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. However, Brandeis, J. dissented and observed that the application of the constitution must contemplate not only what is but what may be. Warning against technological advancements which are furnishing the Government with means of espionage, he expressed regard over the importance of protecting a man's unexpressed beliefs, thoughts and emotions

[46] *Rustom Cavasjee Cooper* v. *Union of India*, (1970) 1 SCC 248.

[47] *Boyd* v. *United States*, 1886 SCC OnLine US SC 58, para 15.

[48] *Meyer* v. *Nebraska*, 1923 SCC OnLine US SC 150. Court struck down a State law that prohibited the teaching of foreign languages to students that had not yet completed the eighth grade. The Court in a 7 : 2 decision, written by McReynolds, J. concluded that the State failed to show a compelling need to infringe upon the rights of parents and teachers to decide on the best course of education for young students.

[49] *Pierce* v. *Society of Sisters*, 1925 SCC OnLine US SC 168. Court struck down the Oregon Compulsory Education Act, which mandated all children (between eight and sixteen years) to attend public schools. It was held that the said statute is an "unreasonable interference with the liberty of the parents and guardians to direct the upbringing of the children, and in that respect violates the Fourteenth Amendment"

[50] *Olmstead* v. *United States*, 1928 SCC OnLine US SC 131.

from Governmental intrusion. The 1967 decision in *Katz* v. *United States*[51] overruled *Olmstead* and revolutionised the interpretation of the Fourth Amendment regarding the extent to which a constitutional right to privacy applies against government interference. It overruled the "trespass doctrine" which tested whether the authority had trespassed on a private location and replaced this doctrine it with the "reasonable expectation of privacy doctrine" which extended the protection of the Fourth Amendment from "places" to "people", affording individuals more privacy even in public.[52] The constitutional question in the case was whether the Fourth Amendment protection from "unreasonable searches and seizures" was restricted to the search and seizure of tangible property, or did it extend to intangible areas such as conversations overheard by others. It was held that the Government's eavesdropping activities violated the privacy, upon which petitioner justifiably relied, while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment, and that the Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements. The reasonable expectation of privacy doctrine was articulated as follows:

"*26. …* "*the Fourth Amendment protects people, not places*". *The question, however, is what protection it affords to those people*. Generally, as here, the answer to that question requires reference to a "place". My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, *first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as "reasonable". Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable*."

The same position has been held in India in *Puttaswamy* wherein it was observed that the right to privacy is attached to the person as essential concomitant of human dignity, and

[51] *Katz* v. *United States*, 1967 SCC OnLine US SC 248. In this case, Charles Katz was a gambler who used a public telephone booth to transmit illegal wagers. Unbeknownst to Katz, the FBI which was investigating Katz's activity, was recording his conversations via an electronic eavesdropping device attached to the exterior of the phone booth. Subsequently, Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights.

[52] *Ibid*, para 6. "...One who occupies it [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is *surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication*." Para 25. ". … (*a*) that *an enclosed telephone booth is an area where, like a home* … a person has a constitutionally protected reasonable expectation of privacy; (*b*) that *electronic, as well as physical intrusion into a place that is in this sense private may constitute a violation* of the Fourth Amendment.…"

would not be lost merely because the individual is in a private place.[53]

The right to privacy in bank records was analysed by the US Supreme Court in *United States* v. *Miller*[54]. In a 6:3 majority, the Court held that the defendant had no right to privacy in his bank records since those records were not his private papers but belonged to the bank as business records and hence no legitimate expectation of privacy could be evinced. It reasoned that cheques were negotiable instruments to be used in commercial communications and thus, all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities.[55] However, Brennan, J. who dissented observed that a bank customer had a reasonable expectation of privacy that his records shall be used by the bank only for internal banking purposes and not be conveyed to third parties or the government. Moreover, such records reveal many aspects of the customer's private affairs, opinions, habits, associations.[56] The existence of dissent in *Miller* points to how the reasonable expectation of privacy test can be subject to many interpretations.

In *Smith* v. *Maryland*[57], it was held that installation and use of a "pen register" (A pen register, or dialed number recorder (DNR), is an **electronic device that records all numbers called from a particular telephone line**) was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required. The court observed that there could be no legitimate expectation of the right to privacy over phone numbers they dial since all telephone users would inevitably have to convey their phone numbers to the telephone company and that all subscribers realise that the phone company has facilities for making permanent records of the numbers they dial which is used to present their monthly telephone bills. Pen registers were also used to identify frauds and in preventing other crimes. Adopting the test of reasonable expectation of privacy, the court noted that:

"*8. ... Since the pen register was installed on telephone company property at the telephone company's central offices, the petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area".*"

Thus the Court held that the petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialled, and that, even if he did, his expectation was not "legitimate". However, Stewart, J. and Brennan, J. who dissented observed that the information obtained by a pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy. The user's conversations from dialing numbers emanates from private conduct within a person's home or office-

[53] *KS Puttaswamy*, para 483. Also see the" Choose and Specify" Test in section 3.2.

[54] *United States* v. *Miller,* 1976 SCC OnLine US SC 70. Federal agents were investigating the defendant for his involvement in a bootlegging conspiracy. The agents subpoenaed two banks and received his bank records. As a result, he was indicted.

[55] *Ibid*, para 14-16.

[56] *Ibid*, para 30.

[57] *Smith* v. *Maryland*, 1979 SCC OnLine US SC 128.

both these places are entitled to Fourth and Fourteenth Amendment protection. Similarly, Marshal, J. who dissented warned against the dangers of surveillance:

"*37. ... Privacy in placing calls is of value not only to those engaged in criminal activity. The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organisations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. ... Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review.*"

In *Kyllo v. United States*[58], the Court considered whether the use of a thermal imager by law enforcement agents constitutes a "search" within the meaning of the Fourth Amendment. The Court held with a 5 : 4 majority that the thermal imaging of the house of a person suspected of growing marijuana was a violation of the right to privacy. Scalia, J. observed that it was impossible for the court to specify which home activities are intimate and which ones aren't and thus, a claim that thermal imaging did not show "intimate details" of the house was held unmaintainable- there is no distinction between "off-the-wall" and "through-the-wall" surveillance as both lead to an intrusion into an individual's privacy.

In *United States* v. *Jones*[59], it was held with a 5:4 majority that installing a Global Positioning System (GPS) tracking device on a vehicle and using the device to monitor the vehicle's movements constitutes a search under the Fourth Amendment. The trespass test was applied in which it was held that the Government's physical intrusion onto the defendant's car for the purpose of obtaining information constituted trespass and therefore a "search". However, the test failed to explain whether GPS data could be obtained without any physical intrusion. Nevertheless in Alito, J. concurrence opinion it was observed that, physical intrusion is now unnecessary to many forms of surveillance, and held that the trespass doctrine would fall short of addressing privacy protections which do not involve physical intrusion into property.[60]

In *Riley* v. *California*[61], the court unanimously held that the search and seizure of digital contents of a cell phone without a warrant and during an arrest is unconstitutional. Roberts, C.J. observed that a search on the phone was not limited to physical intrusion of privacy, and permeated

[58] *Kyllo* v. *United States*, 2001 SCC OnLine US SC 61.
[59] *United States* v. *Jones*, 2012 SCC OnLine US SC 13.
[60] The court also warned against the dangers of making GPS data accessible at the hands of law enforcement: "… The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and Government in a way that is inimical to democratic society."
[61] *Riley* v. *California*, 2014 SCC OnLine US SC 71.

to the data on the phone. The data on the phones and particularly smart phones usually contain historical locational information of the person even within a building which can enable authorities to reconstruct every minutiae related to the person's movements. Even application softwares on mobile phones reveal a great deal of personal information. The court observed:

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life"…. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."

The evolution of the right to privacy in the USA is older than India's own jurisprudence on the matter. India and the USA have both made implicit interpretations of the right to privacy among fundamental rights and liberties guaranteed in Part III and the Bill of Rights respectively. However, in addition to the Fourteenth Amendment protection of due process, the Fourth Amendment requirement is a stronger safeguard against "search and seizure" than India's own safeguards implicitly read into "procedure established by law" contemplating a standard of reasonableness. Although the Fourth Amendment also necessitates a requirement of reasonableness as evidenced from the words "probable cause" which appear in the Amendment, it still assertively holds that no "search or seizure" can take place warrantless. The requirement of a prior authorization to surveil someone by means of a warrant makes American constitutional safeguards more adept. Yet again, the requirement of a warrant for any "search and seizure" is not absolute, American courts have made some exceptions to this.

Although, the CRPC also provides for a requirement of warrants to conduct searches, the meaning of "search and seizure" as is understood from the CRPC cannot include surveillance, unlike in the Fourth Amendment where "search and seizure" has not only been broadly defined to include non-physical searches but also extended to rapidly evolving technologies which have made surveillance more pervasive in citizens' lives. In India, the courts have allowed many instances of surveillance whilst also correspondingly recognizing a right to privacy. Since American jurisprudence relies on the reasonable expectation of privacy test, the courts have proceeded to determine the validity of a privacy intrusion on that ground alone- this is an individual centric approach. However, in India, the limitations on the validity of a privacy intrusion have been defined more by the compelling state interest doctrine, which has sought to sustain the effects of surveillance insofar as the state has enacted substantive and procedural safeguards within the impugned law- this is a state centric approach.

It is important to note that the Court in *Puttaswamy* has held that information which is already in public domain is not amenable to privacy protection if voluntarily parted with, relying on the *Miller* judgment of the US SC. Information already in public would still warrant privacy protection from the choose and specify test, when any information is made public, it is made public for a specific purpose and its use beyond such

purpose would be a function creep. This is the logic on the basis of which the dissent in *Miller* proceeded from. However, in *Puttaswamy* not preferring the dissent in *Miller*, has taken a narrow view of privacy.

The Indian court has also practiced the doctrine of judicial deference more in this sphere, perhaps curtailed by 'national security interests', and has not been able to take a proactive stance against surveillance.

4. SURVEILLANCE IN INDIA

Surveillance through census in the British Indian period changed the nature of communal conflicts. What was originally understood as sectarian conflicts between two groups became a conflict between two nations (the Hindus) and the foreign "other" (non-Hindus). By then philosophical discussions and debates on religion had become unimportant, and community wise numbers which the censuses evinced became an important source of communal conflict- for instance, how many Hindus are there as against the Muslims? Such is the impact of surveillance. Colonial state administrations resorted to surveillance to replace their methods of direct violence on the subject population, since it made the subjects hostile and noncooperative. Colonial regimes developed sophisticated forms of control through documentation and surveillance- particularly in British colonies to control and monitor "dangerous populations" by means of traveling passes, distinctive zones, and permit regimes. An author has noted,

"*As the technologies of population management shifted from the colonies back to the metropole, they ensconced the administrative structures of colonial bureaucracy. Colonial bureaucracy was founded on emergency laws and used separate racialized practices for different populations. It produced constant administrative exceptions, uncertainties, and what I call "effective inefficiency" designed to slow down the movement of the population.*"[62]

The conception of surveillance has expanded beyond particular individuals and changed into arbitrary mass surveillance and beyond the purposes of crime prevention and all this occurs through evolving new technology which the law and the courts have yet to account for.

The centralized monitoring system in India has been labelled as the Indian PRISM- is an obscure government program. The CMS provides that "Every call made either from a landline or mobile phone can be listened to and its location fixed. All text messages, emails and searches on the internet can be collated and analysed."[63]

The Central Intelligence Network ('CIN') was a proposal from the NIA which sought to allow lateral surveillance which uses citizens' volunteership in the intelligence gathering mechanism to help prevent terrorist strikes in the country.[64]

The Indian Telegraph Act 1885, which is a law from the British Raj, governs the

[62] Yael Berda, 'Managing Dangerous Populations: Colonial Legacies of Security and Surveillance', 28(3) (2013) *Sociological Forum*, 627–630 <www.jstor.org/stable/43653901> accessed 24 Apr 2021.

[63] SAHRDC, 'Architecture of Surveillance' 49(1) (2014) *Economic and Political Weekly*, 10–12 <www.jstor.org/stable/24478446> accessed 24 Apr 2021.

[64] *Ibid.*

government's access to communication data and interception. The Act allows interception of messages between citizens only on grounds of 'public emergency' or 'public safety'.[65]

The Information Technology Act is largely responsible for surveillance as well as surveillance induced censorship. The IT Act does not even require standards of 'public emergency' or 'public safety' to intercept messages and content on the internet. A scholar has noted thus, "*While replicating most of these provisions from the Telegraph Act into the 2008 Amendment Act, the drafters did away with the preconditions of public emergency or public safety, thus lowering standards for accountability. Further, these two co-existing laws are inconsistent and contain varying standards on the types of interception allowed, destruction and retention requirements of the material intercepted, permitted grounds of surveillance, degree and measures of assistance that authorised agencies can demand from the service providers.*"[66] This inconsistency is set to cause an unclear regulatory regime with no transparency. Section 69 of the Act allows the government to intercept and watch over electronic communications in order to investigate any offence regardless of its gravity and has also expanded its ambit to include any information and correspondences being sent or received via the internet.[67] This enables the decryption of information. Sections 69A and 69B enable the monitoring and procurement of information and correspondences that are a "probable threat (to the sovereignty or integrity of India, defence of the country, security of the state, foreign relations or are capable of the incitement of any cognisable offence), is by means of setting up content filters or 'packet sniffing programmes' on the internet. These content filters search for specific terms in the correspondences taking place over the internet, such as 'kill', 'Lashkar-e-taiba' and the like. Once a correspondence of this nature is intercepted, regardless of its context the sender or receiver or both will be under surveillance."[68] The court in *Shreya Singhal* upheld section 69 whilst providing safeguards against abuse. The court specified that blocking orders would have to be in writing and the reasons for the same have to be mentioned therein, and that blocking orders would be subject to writ proceedings.

The Unique Identification Authority of India ('UIDAI') has now served to produce a systematic basis for technological surveillance, initially it was established to provide poor people with an identity so they could avail benefits, however, it has lead to an exclusion of many marginalized for not have documentary proofs to prove their identity.

Agencies like National Intelligence Grid ('NATGRID') and the Crime and Criminal Tracking Network have been set up. Wide ranging data relating to an individual's travel, taxes, religion, marital status, disability, DNA, etc. is collected by the agency through communication technology.

[65] Editorial Note, on Censorship and Surveillance, 7 NUJS Law Review (2014).
[66] *Ibid.*
[67] Sakshi Sawhney, 'The Information Technology (Amendment) Act, 2008 : The Provenance of E-Policing', 5 NSLR (2010) 160.
[68] *Ibid.*

The COVID-19 induced public health surveillance is also a deep cause of concern. It is feared that citizen tracking and mass health collection data can outlast the pandemic and become part of our daily lives. Two tools are being used- "personnel tracking GPS solution" and a "COVID-19 patient tracking tool". The Internet Freedom Foundation of India has assessed that these tools pave way to mass surveillance. Similarly, the Internet Freedom Foundation has also assessed a new policy of the UP police called 'Hamari Suraksha' in which people viewing porn websites which show child sexual abuse material (CSAM) will be shown pop up messages to sensitise them against viewing it, which will be done through AI and psychographics. This policy lacks any legal framework which can result in Function creep;[69] there is no clarity on how user's privacy will be protected if IP addresses are to be collected and stored- it can lead to a targeting of all pron which would result in a violation of freedom of speech and expression, the policy also fails to fulfil the proximity test because people will simply find new ways of viewing CSAM like VPNs- the best outcome would be for the UP Police to find websites hosting such content and take them down and prosecute them under existing laws like IT Act and POCSO.

The IT Rules of 2021 are also another cause of concern. In most recent times, surveillance has begun to occur through intermediaries- "entities that provide services enabling the delivery of online content to the end user. They include Internet Service Providers (hereinafter 'ISPs') who enable internet connections, search engines, web hosts, interactive websites (social media sites, e-commerce or auction sites, payment gateways and blogging platforms among others), Domain Name System (hereinafter 'DNS') providers and even cyber cafes."[70] Although the rules have positive provisions like requiring authorities to give an explanation to users for removing online content, notices to be given to users before their accounts are suspended, social media firms have to furnish compliance reports; the criticisms outweigh the positives. The Rules have been couched in vague language which will have a chilling effect, censoring both lawful and unlawful speech. Since the language is vague and overbroad, short timelines of social media companies to file compliance reports will result in over compliance enabling them to take down or block content more frequently. The Rules also provide for a tracking mechanism for every message, which can obliterate end to end encryption and pave the way to surveillance capitalism. Automated tools like "packet sniffing programs" which will review certain "offensive" keywords and block them. This has purveyed too much power to the government ministries to block, delete or modify content on news and OTT platforms. Its ramifications on digital news platforms are huge, and is currently being challenged in the SC by journalists on the account of the infringement of the freedom of the press. These news platforms face a threat of content blockage and removal if they do not comply with the government's orders thereby effectively silencing dissent.

The facial recognition technology which is becoming increasingly pervasive is another mode of mass surveillance. An Aadhaar

[69] Where the function of a deployed technology starts being widened beyond its original scope.

[70] Smriti Kanwar, 'Simple Amendments, Clipped Democracies and No Privacy - Need for Informed Participation', 6 CMET (2019) 1.

based facial recognition system is now being proposed to replace biometric fingerprints or iris scan machines at COVID-19 vaccination centres to avoid infections from contact. It is being feared that it will result in exclusion and discrimination since subjecting access to COVID19 healthcare to facial recognition will increase risks of exclusion since facial recognition technology ('FRT') is not always accurate; the use of FRT violates our right to privacy; there are also chances of function creep. The Internet Freedom Foundation has recognized two reasons why FRT is being increasingly deployed by governments: one, for security and surveillance by means of a single database which stores data on faces of all Indian citizens and is used to match the individual's face to information that government already has by the police; two, for automatic identity verification of citizens wherever they go- in schools, offices, polling stations. There are several problems associated FRT: one, there is no legislative framework which sanctions it, and therefore, there exists no mechanism which can hold the government accountable where anyone can gain access to citizens' facial recognition data; two, FRT works through AI which maps several little points on your face and saves those points as data, this data is then used to correspond with other images and videos to place your identity- the problem is that FRT in India is below average which increases scope for mismatch, and the tech can wrongly identify an innocent person as the one who is being searched for a crime committed- it can also fail to recognize your identity where it is needed and deny access to resources; it can have panopticon function and thus, people will be self censoring wherever there is FRT.

5. WAY FORWARD

Whenever there are surveillance systems in place, there are three questions that ought to satisfied:

(i) Is the surveillance system warranted under existing law?

(ii) Is its need necessary and proportional to the object being sought to be achieved?

(iii) Even if it is proportional, are there procedural safeguards against function creep?

India currently has a Data Protection and Personal Privacy Bill in the making. The Bill seeks to regulate three categories of persons-

(i) the Data principal, who is the owner of the data;

(ii) the Data Fiduciary, who stores the data like Facebook, Google and government bodies; and

(iii) the Data Processor, who uses the data like healthcare professionals or advertisers.

The information that is sought to being meted out from the Data principal are sensitive/personal data which includes details of a persons' name, phone number, address, caste, tribe, religion, sex, sexuality, political beliefs, DNA, iris, fingerprints, etc. Although the Bill emphasizes consent of the principal in divulging data and the right to know and be informed about any data breaches, how your data is being used and by whom, and the decision to withdraw consent; in practice this consent has been made excessively and vaguely conditional. For instance, if one has to withdraw consent- they must furnish valid reasons why they don't want their data to be processed anymore and if they fail to do so, they may face legal consequences. The Bill does not clarify what reasons are valid and would be such “legal consequences”. Moreover, a fee must be paid in withdrawing consent. This will prevent citizens from

exercising their constitutional rights. Another instance is that several exceptions have been created where consent is not required- where the government wants to give you services; however, this has been enabled without any adequate checks and balances. Under the Bill, even an employer can access personal data of their employees. Moreover, consent is not required to use our data if such data is publicly available. Unfortunately, in the internet age, so much personal data is publicly available- so without any prior authorization of the Principal, the government can use this information to discriminate citizens on political and religious grounds, and force profiling and political ads upon us. This is contrary to the choose and specify test. Although a person's personal data may be available on social media, this does not mean that the principal expects their information to be accessed by someone they have specifically excluded from accessing. The Bill also undermines anonymity by providing a clause which makes verification voluntary. This means verification would require indulging in details such as Aadhaar ID or the like, which will now grant more access to the social media company to more sensitive data. The Data Protection Authority ('DPA') is not autonomous and a government inclined bias can be expected, the DPA is bound by the directions of the Central Government.

There is a need to undertake wider-publicized awareness about digital rights of the citizens. This is important to enhance more meaningful public engagement in the legislative process. Surveillance has a direct impact on not only privacy but all other personal liberties connected therewith, and thus, such engagement is meant to help citizens fulfil their responsibilities under the constitution through democratic participation. Users of technology are not merely consumers of information but also co-creators of information, and thus, data protection related public engagement must address privacy and freedoms concerned at both these levels.

More importantly, these surveillance scales are occurring in a regime without any legislative framework- which is patently violative of the "procedure established by law" requirement under Article 21. The subsistence of contradictory and inadequate regulatory regimes of content over the internet in the absence of a data protection law exhibits that a matter of such scale concerning privacy is currently being handled by the executive wing of the government through notification of Rules and orders without any Parliamentary oversight, this has purveyed arbitrary powers to the government Ministries. One of the contentions of the journalist-petitioners who have challenged the IT Rules had been that the IT Act does not seek to regulate "news intermediaries" and therefore, the use of vague terms is a case of excessive delegation and ultra vires the scope of the parent Act. And thus, a law is needed which incorporates specific and binding provisions for transparency and accountability mechanisms like that which requires full disclosure of reasons in writing before any content is sought to be blocked or removed, and a citizen redressal mechanism against such orders of the government before an independent authority. Another recommendation which has come by is that the Departments and agencies of the government seeking citizens' information must publicly disclose the reasons for the same and make known to the public how their

data is being processed by the governments through compliance reports which will be assessed by an independent authority and scrutinized by the public. And exemptions from disclosure on 'national security' grounds should be allowed only under a law which cogently and narrowly defines the scope of exemption.

REFERENCES:

[1] Daniel J Solove, 'A Taxonomy of Privacy', 154 (3) (2006) University of Pennsylvania Law Review, 477-560 <A Taxonomy of Privacy by Daniel J. Solove :: SSRN> accessed 18 April 2021.

[2] Gautum Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution*, (Oxford University Press, 2018).

[3] *K S Puttaswamy (Privacy- 9J) v Union of India*, (2017) 10 SCC 1.

[4] *Shreya Singhal v Union of India*, (2015) 5 SCC 1.

[5] Smriti Kanwar, 'Simple Amendments, Clipped Democracies and No Privacy - Need for Informed Participation', 6 CMET (2019) 1.

[6] Editorial Note, on Censorship and Surveillance, 7 NUJS Law Review (2014).

[7] Sakshi Sawhney, 'The Information Technology (Amendment) Act, 2008 : The Provenance of E-Policing', 5 NSLR (2010) 160.

[8] Yael Berda, 'Managing Dangerous Populations: Colonial Legacies of Security and Surveillance', 28(3) (2013) *Sociological Forum*, 627–630 <www.jstor.org/stable/43653901> accessed 22 Apr 2021.

[9]SAHRDC, 'Architecture of Surveillance' 49(1) (2014) *Economic and Political Weekly*, 10–12 <www.jstor.org/stable/24478446> accessed 24 Apr 2021.

[10] Otis H Stephens, Jr., John M. Scheb, *American Constitutional Law: Civil Rights and Liberties* (Vol II, 4th edn., Thomson Wadsworth 2008).

[11] Chinmayi Aru, 'PAPER-THIN SAFEGUARDS AND MASS SURVEILLANCE IN INDIA' 26(2), (2014) National Law School of India Review, 105-114 <www.jstor.org/stable/4428363> accessed 12 March 2021.

[12] Bedavyasa Mohant, 'Inside the Machine: Constitutionality of India's Surveillance Apparatus', 12 IJLT (2016) 206.

[13] Binoy Kampmark, 'The Pandemic Surveillance State: an Enduring Legacy of COVID-19', 7(1) Journal of Global Faultlines, 59–70 <www.jstor.org/stable/10.13169/jglobfaul.7.1.0059> accessed 22 Apr 2021.

[14] Mrinal Satish, 'Bad Characters, History Sheeters, Budding Goondas and Rowdies': Police Surveillance Files and Intelligence Databases in India', 23(1) (2011) National Law School of India Review, 133–160 <www.jstor.org/stable/44283744> accessed 23 Apr 2021.

[15] Janaki Bakhle, 'Savarkar (1883–1966), Sedition and Surveillance: the Rule of Law in a Colonial Situation', 35(1) (2010) *Social History*, 51–75 <www.jstor.org/stable/25677339> accessed 23 Apr 2021.

[16] Shamsi, Hina, and Alex Abdo, 'Privacy and Surveillance Post-9/11', 38(1) (2011) *Human Rights*, 5–17 <www.jstor.org/stable/23032368> accessed 23 Apr 2021.

[17] Tarafder, Agnidipto, 'SURVEILLANCE, PRIVACY AND TECHNOLOGY: A COMPARATIVE

CRITIQUE OF THE LAWS OF USA AND INDIA', 57(4) (2015) Journal of the Indian Law Institute, 550–578 <www.jstor.org/stable/44782800> accessed 23 Apr 2021.

[18] Jadallah, Alma Abdul-Hadi, 'CIVIC SPACE IN INDIA: BETWEEN THE NATIONAL SECURITY HAMMER AND THE COUNTERTERRORISM ANVIL', edited by Lana Baydas and Shannon N. Green, Center for Strategic and International Studies (CSIS), (2018) COUNTERTERRORISM MEASURES AND CIVIL SOCIETY: Changing the Will, Finding the Way, 61–72 <www.jstor.org/stable/resrep22446.9> accessed 23 Apr 2021.

[19] Acharya, Bhairav, 'The Four Parts of Privacy in India', 50(22) (2015) Economic and Political Weekly, 32–38 <www.jstor.org/stable/24482489> accessed 24 Apr 2021.

[20] Singha, Radhika, 'Punished by Surveillance: Policing 'Dangerousness' in Colonial India, 1872–1918', 49(2) (2015) Modern Asian Studies, 241–269 <www.jstor.org/stable/24495402> accessed 24 Apr 2021.

[21]Gautum Bhatia, 'STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BIOGRAPHY', 26(2) (2014) National Law School of India Review, 127–158 <www.jstor.org/stable/44283638> accessed 24 Apr 2021.

*****