AN ARMISTICE BETWEEN RIGHT TO PRIVACY AND RIGHT OF SURVEILLANCE

*Varun Kalra and Ramisha Jain**

ABSTRACT

The Supreme Court on 24 August, 2017 upheld the Right to Privacy.[1] Despite this proclamation, a major question remains still unanswered that "What does privacy mean for India".

"What would be the impact of the change in WhatsApp's privacy policy on the users? Is Aadhar a surveillance mechanism? These are the issues which are still dominating the cause list of Supreme Court of India today. The Indian Judiciary has recently answered a question which will have a lingering effect on the Indian democracy, that is, do the Indian citizens have a right to privacy? According to Black's law dictionary, right to privacy is, "right to be let alone; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned". However, this right has been in conflict with the right of surveillance by the sovereign since time immemorial. And since the announcement of the Aadhar Card Scheme, the tussle between the two has been gaining ground.

This paper aims at critically analysing the legal position of right to privacy in India by tracing the case- by- case development of this newly acknowledged right. Also, this paper seeks to discuss the controversies involving the right to privacy, understand the need for a comprehensive privacy policy and to assess the use and abuse of right of surveillance. The object of this paper is to offer recommendations to end the tussle between the right to privacy and right of surveillance, by clearly laying down the restrictions on right to privacy, by recognising surveillance agencies and providing for a code to limit and prevent the abuse of their powers and ultimately, establishing an interface between the right to privacy of the citizens of India and the right of surveillance by the government of India.

INTRODUCTION

The Ghost of Christmas Past, Right to Privacy, had decided to reappear with the Aadhar case.

* Authors are fourth year B.A.LLB. (Hons.) students at Amity Law School, Noida.

[1] Justice K.S. Puttaswamy and Ors. v. Union of India (UOI) and Ors., (2017) 6 MLJ 267.

Not only did this issue once again sparked off the debate that whether the right to privacy is guaranteed under Article 21 of the constitution or not, but had also renewed the fierce battle between right to privacy and right of surveillance.

With the recent change in WhatsApp's privacy policy, questionable use of information by UIDAI and the growing tussle between the government agencies for more lethal surveillance systems, demand for privacy and freedom of speech and expression has been gaining ground. The right of privacy of the citizens and the right of surveillance of the State are once again at loggerheads.

The need for privacy flows from the growing individualistic society, a modern phenomenon.

According to *Black's Law Dictionary*, right to privacy is, "right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned".

As per Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Right to Privacy is guaranteed in the American Constitution under the Fourth Amendment. The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause. It is part of the Bill of Rights and was adopted in response to the abuse of the writ of assistance, a type of general search warrant issued by the British government and a major source of tension in pre-Revolutionary America.

However, until recently, there was no such explicit guarantee, under the Indian Constitution or so it was argued. According to Article 21, "No person can be deprived of his life and personal liberty except according to the procedure established by law". The question is whether Right to life and Personal Liberty include the Right to Privacy.

Amidst the controversy between National Security and the Fundamental Rights of the people, it's the Indian citizen who is in a no-win situation.

It is a widespread idea that terrorism is a product of globalization and the Internet is a tool used by the terrorists to communicate. Hence governments all around the world believe that surveillance is the most effective methods

of detecting and prosecuting terrorists. All the movements, actions, interests, ideas and everything else that could define a common man or an individual can be known by surveillance. Mass-surveillance as we know today has been in practice since many years. Today, whatever we do, from the moment we switch on our cell phones, to navigating to a location using Google Maps, to catching a metro/bus with CCTV cameras, to using our credit cards for an online or offline purchase, we leave a digital trail behind us. The government is capable of knowing our medical history, routine, preference of food, religion, places of visit, the movies we watch, the place we shop from, what we purchase, whether we are having an affair or not, everything. All these things are easily accessible through our digital trails, some of which we ourselves provide to them by updating our statuses on WhatsApp, Snapchat, Facebook etc. It is the appalling truth behind constant surveillance that the government carries out on us.

Moreover, with the global surveillance disclosures, right to privacy has become a subject of international debate. To combat terrorism, government agencies are undermining this right. Another question which now needs answering is that whether privacy needs to be forfeited as a part of social contract. Hence, it is of utmost importance that the battle between the two above stated rights is brought to an end.

RIGHT TO PRIVACY IN INDIA AND ITS LEGAL POSITION

Right to Privacy is not enumerated in the Indian Constitution, but the Indian Judiciary has from time- to- time debated on the existence of this right in the Indian Legal Framework and has culled the same from Article 21.

(A) 1950- 2000

In, *M. P. Sharma v. Satish Chandra*[2], it was held that, when the constitutional makers themselves did not recognise the fundamental right to privacy, then an analogy needn't be drawn with American Constitution in order to import this right "by some process of strained construction" and thus, the existence of right to privacy in India was denied.

However, in *Kharak Singh v. State of UP*[3], the apex court while acknowledging the existence of right to privacy held that, despite the right not being expressly declared as a fundamental right, it is "an essential ingredient of personal liberty". The legal position of the disputed right was upheld in *Gobind v. State of Madhya Pradesh*[4], wherein the bench held that "*the right to privacy in any event will necessarily have to go through*

[2] AIR 1954 SC 300.
[3] AIR 1963 SC 1295.
[4] AIR 1975 SC 1378.

a process of case-by-case development." Mathew, J. accepted "the right to privacy as an emanation from Art. 19(a), (d) and 21, but right to privacy is not absolute right." Reiterating the same in *R. Rajagopal v. State Of T.N.*[5], or better known as the Auto Shanker case, it was held that "*A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. No one can publish anything concerning the above matters without his consent, whether truthful or otherwise whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in the action of damages*."

(B) 2000-2016

It was held in *Sharda v. Dharampal*[6] that the right to privacy is subject to restrictions. It is not enshrined in the Indian Constitution but has been drawn out from the extensive interpretation of article 21. Also, in *District Registrar and Collector, Hyderabad and another v. Canara Bank and another*[7], another two-Judge Bench held, while accepting the implicit existence of right to privacy in India, that the right to privacy dealt with persons and not places. One of the most prominent and recent case dealing with right to privacy is *Ram Jeth Milani v. Union of India*[8], wherein the ratio of the case was *"Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner."* Another recent landmark judgement on the same is of *Amar Singh v. Union of India*[9], where it was upheld that it was the Court's duty to protect the right to privacy. Also in *Thalappalam Ser. Coop. Bank Ltd. and Ors. v. State of Kerala and Ors*.[10], the honourable Court held that right to privacy falling under Article 21 of the Indian Constitution is not absolute and needs to regulated in public interest as in the modern state, no right can be absolute. But it was finally in the Aadhaar card case i.e. *Justice K.S.Puttaswamy(Retd)& Anr v. Union Of India & Ors*.[11], it was suggested that in order to settle the legal position of the right to privacy,a constitutional bench must be established.

(C) 2017

The Apex Court on 24th August, 2017, while reaching out to the foundation of constitutional

[5] AIR 1995 SC 264.
[6] AIR 2003 SC 3450.
[7] (2005) 1 SCC 496.
[8] 4 July, 2011, Supreme Court of India.
[9] 11 May, 2011, Supreme Court of India.
[10] 2013 SCJ 7 862.
[11] 11 August, 2015, Supreme Court of India.

culture of India, proclaimed Privacy as a postulate of human dignity. They acknowledged that privacy lies across the spectrum of protected freedoms and is the ultimate expression of the sanctity of an individual. While commenting on the nature of privacy, the Court ruled that while the individual is entitled to a zone of privacy, its extent is based not only on the subjective expectation of the individual but on an objective principle which defines a reasonable expectation. Inspite of having settled the legal position of this much disputed, a comprehensive privacy policy is needed to establish a delicate balance between the legitimate concern of the State and individual interest[12].

RECENT CONTROVERSIES ON RIGHT TO PRIVACY

Currently there are many cases and appeals pending in various courts in India the substratum of which is the right to privacy.

Firstly, in the **Naz Foundation** case, the Apex Court of India, is hearing a curative petition on § 377 of Indian Penal Code, which criminalises consensual homosexual sex between adults. The section reads as follows: "Whoever voluntarily has carnal inter-course against the order of nature with any man, woman or animal, shall be punished with [imprisonment for life], or with impris-onment of either description for a term which may extend to ten years, and shall also be liable to fine."[13]

The High Court of Delhi in 2009, decriminalised consensual homosexual sex in *Naz Foundation v. NCT of Delhi*[14] and held, *"The sphere of privacy allows persons to develop human relations without interference from the outside community or from the State. The exercise of autonomy enables an individual to attain fulfilment, grow in self-esteem, build relationships of his or her choice and fulfil all legitimate goals that he or she may set. In the Indian Constitution, the right to live with dignity and the right of privacy both are recognized as dimensions of Article 21. § 377 IPC denies a person's dignity and criminalizes his or her core identity solely on account of his or her sexuality and thus violates Article 21 of the Constitution. As it stands, § 377 IPC denies a gay person a right to full personhood which is implicit in notion of life under Article 21 of the Constitution."*

However, the Supreme Court of India, in appeal, overturned the judgment of the Delhi High Court in the case of *Suresh Kumar Koushal &*

[12] Justice Puttaswamy (Retd.) and Anr. v. Union of India and Ors., W. P. (C) No. 494 of 2012 and W. P. (C) No. 000372/2017, 24 August, 2017, Supreme Court of India.

[13] Indian Penal Code (45 of 1860), § 377.

[14] 160 Delhi Law Times 277.

Anr vs Naz Foundation & Ors[15].

In 2014, the Supreme Court, in a landmark judgement, directed the government to treat the transgenders as the 'third gender' and to include them in the OBC quota. But the matter pertaining to § 377 is still pending.

Secondly, the **Aadhar Card** scheme has been under attack ever since its institution. However, the Apex Court, in the case of *Justice Puttaswamy v. Union of India*[16], quelled the debate for a while by holding that the information obtained by the authorities will have restricted use i.e. for PDS Scheme, and will not be sued for any other purpose, except by the leave of the court for the purpose of criminal investigation. Further, it recommended the institution of a constitutional bench to determine the legal position of right to privacy. Yet, after some time, the Aadhar card issue reared its head again. It is being referred to as an undemocratic way which is being used to take away the right to privacy. Many believe that Aadhar Card Scheme is being converted into the world's biggest surveillance system by obtaining biometric and linking the card to services such as filing of Tax Returns, Bank Accounts etc. A constitutional bench headed by the then CJI, H.L. Dattu, held that Aadhar card is to be voluntary and not mandatory, however, it is being made mandatory for certain schemes, for example it has been made mandatory for availing of minority students' scholarships. In some ways, the policy decisions around Aadhar can be seen as illustrative of erosion of Parliament, for ex., Money Bill aspect of Aadhar card. Moreover the Standing Committee of Finance of 15th Lok Sabha had observed that the scheme was "ladled with lacunae" and was ambiguous. The Committee was of the opinion that a comprehensive privacy law is a prerequisite of the scheme. It is also an erosion of the rights of the citizens. Despite the defence and clarifications offered by Nandan Nilekani, the brain behind the UIDAI, it can be seen that this scheme is not only questionable but has failed on several metrics. Recently, the Aadhar details of 10 lakh citizens were made public by Jharkhand Directorate of Social Security due to a programming order, which further fuelled the debate surrounding the scheme.

Thirdly, the **WhatsApp Controversy**, Karmanya Singh Sareen and Shreya Sethi had filed a PIL with respect to change in privacy policy of WhatsApp without informing users which does not amount to fair practice and is moreover, hit by the principle of estoppel. WhatsApp, after being acquired by Facebook had started sharing the information of the users with Facebook in order to improve advertisements and product service. A bench of

[15] 11 December, 2013.
[16] 11 August, 2015, Supreme Court of India.

the Delhi High Court headed by the then CJ G. Rohini, granted partial relief and ordered WhatsApp to delete all the user information till 25 September, 2016, however, the bench did not declare the sharing of information by the enterprise in the future as illegal by stating that the users who do not wish for their information to be shared to opt for the deletion of WhatsApp account. An appeal was filed with respect to the latter part of the judgment, which is currently pending before the constitution bench of the Supreme Court.

LEGISLATIVE ATTEMPTS TOWARDS SECURING RIGHT TO PRIVACY

There have been various legislative attempts to secure the right to privacy, however, they have not been very successful. *Firstly*, as per the **Information Technology Act, 2000,** when a body corporate fails to protect personal data it owns or controls, such body corporate shall be liable to pay damages by way of compensation[17].

*Secondly***, Venkata Challiah Commission**, the National Commission to review the working of the Constitution (NCRWC) also known as Justice Manepalli Narayana Rao Venkatachaliah Commission was set up on 22 February 2000 for suggesting possible amendments to the Constitution of India. The commission recommended the insertion of Article 21B in the Indian Constitution, which would read as follows:

"21-B. (1) Every person has a right to respect for his private and family life, his home and his correspondence.

(2) Nothing in clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the State, public safety or for the prevention of disorder or crime, or for the protection of health or morals, or for the protection of the rights and freedoms of others."[18]

Unfortunately, it took fifteen years from the date of submission of this report to accept Right to Privacy as a Fundamental Right, and yet, a comprehensive privacy policy is yet to be devised.

Finally, despite there being three **Right To Privacy Bills,** neither of the bills have been given the status of a statute. As per the bills, Right to privacy could not be infringed except according to provisions of the act or law. The grounds for infringing the right to privacy included: (a) sovereignty and security of India,

[17] Information Technology Amendment Act, 2008, § 43A.

[18] Justice Venkata Challiah Committee Report, Vol. 1, 3.12, http://lawmin.nic.in/ncrwc/finalreport/v1ch3.htm.

technical and economic interests (b) preventing incitement to the commission of an offence (c) prevention of public order or for detecting crime (d) protection of freedom and rights of others (d) in the interest of friendly relations with foreign states (e) any other purpose specifically mentioned in the act[19]. As per the bills, (a) collection, storage, processing and disclosure of personal data, (b) interception or monitoring of communication of individuals, (c) surveillance of individual constitute the infringement of right to privacy[20]. Provisions were made for the establishment of Data Protection Authority of India, National Data Control Registry and Appellate Tribunals. Penalties for violating right to privacy have also been incorporated in the bill, for example, penalty for undertaking surveillance in certain cases would be imprisonment for five years.

NEED FOR A COMPREHENSIVE PRIVACY POLICY

Democracies survive on a delicate balance of power between the government – and the citizens. The more power citizens get, the more robust the democracy. As the government accrues more power to itself, it erodes democracy to a point where it ceases to exist. Thus, privacy is essential to a democracy as it provides for personal autonomy, gives an opportunity for emotional release and self-evaluation. Therefore, there's a need for a comprehensive privacy policy. *Firstly*, to offer **protection from surveillance, search and seizure.** The issue of protection from surveillance was dealt with in Kharak Singh v State of UP[21], wherein the Police abused its power of surveillance, by forcibly entering the plaintiff's house and searching it, keeping a close watch on him, dragging him at times to the police station etc. Hence, the citizens need to be protected from such arbitrary exercise and abuse of power.

Secondly, for the **privacy of the body.** The citizens have an exclusive right over their body, they need to be given the liberty to choose and decide what's correct for them. For example, the Medical termination of Pregnancy Act prevents a woman from exercising her right of abortion by permitting abortion under certain circumstances only. The other issues which fall under the ambit of Medical Privacy are: the ability of the state to order persons to undergo medical-examination and to submit to DNA testing in civil suits, to undergo a range of 'truth technologies' including narco analysis, brain mapping, etc., *Thirdly,* to **Protect reputation.** This issue emanates from the Auto Shanker

[19] Right to Privacy Bill, 2011.
[20] *Supra.*
[21] AIR 1963 SC 1295.

case[22]. With the growing technology and increasing role of media, a mechanism for the protection of reputation is of utmost importance. And *finally,* for the **protection of records, communication and protection from interception in the digital age:** It was in People's Union for Civil Liberties v. Union of India[23], or better known as the Telephone-tapping case, that the question of intimate and confidential nature of communications was brought under the scanner, and the right to privacy was upheld. Therefore, in this digital age, with the increasing rate of cybercrime, a comprehensive privacy policy is inevitable.

SURVEILLANCE

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

— Edward Snowden

When in 2013, the whistle-blower contractor of USA's National Security Agency (NSA), Edward Snowden, quivered the world by disclosing the extensive global surveillance programs by the US Government; the worldwide perception of the common man, that even the world's largest democracies are free from governmental interference was shattered. Little did we know that even India had its own surveillance program, like NSA, since 2007. It enables the Indian Government to keep track in real time of 900 million mobile phones and landlines and 160 million internet users.

STATE AGENCIES AND SURVEILLANCE ORGANISATIONS

After the perturbing 26/11 terrorist attacks in Mumbai, the government of India introduced many data sharing and surveillance systems. The data sharing schemes being the National Intelligence Grid (NATGRID) and the Crime and Criminal Tracking Network & Systems (CCTNS) while the surveillance systems being the Central Monitoring System (CMS), Lawful Intercept and Monitoring (LIM) system and the Network Traffic Analysis system (NETRA) and many other state Internet Monitoring Systems. The purpose of these bodies is to increase public safety and national security by tackling crime and terrorism.

National Intelligence Grid (NATGRID) is an intelligence grid which will consolidate data gathered from various agencies and will link the databases of various departments and ministries of the government of India. It will serve as a one-stop shop for accessing the linked data by the intelligence agencies. Under NATGRID, 21 sets of databases will be networked to achieve

[22] AIR 1995 SC 264.
[23] (1997) 1 SCC 30.

quick, seamless and secure access to desired information for intelligence/enforcement agencies[24]

Crime and Criminal Tracking Network and System (CCTNS) on the other hand is a network that allows the collection, storage, retrieval, analysis, transfer and sharing of information relation to crimes and criminals across the country.[25] Since there used to be no database for the police officers to refer to, to gather and share any information about a criminal and store it virtually, CCTNS was implemented as an ambitious scheme by the Government of India, to maintain a record of crimes and criminals and to share the information with other police stations using computer and maintaining a connectivity between various police stations creating a hub of criminal information collected and stored by various police officers.[26] The access of the same will be provided to the police stations and to intelligence and national security agencies.

Central Monitoring System (CMS) is an interception system that enables government agencies to intercept communications without requiring court orders or needing to communicate with the telecom service providers. It is the most important surveillance system that monitors text messages, social-media engagement and phone calls on landlines and cell phones, among other communications. Once fully implemented, CMS will allow the government to "listen and tape phone conversations, read e-mails and text messages, monitor posts on Facebook, Twitter, or LinkedIn, and track searches on Google."[27] It will also empower the government to keep a real time track of our whereabouts using GPS embedded in our mobile phones.

Lawful Intercept & Monitoring (LIM) Systems were deployed by the Government of India to monitor records of voice, SMS, GPRS data, details of a subscriber's application and recharge history and call detail record (CDR), emails, web browsing, Skype and any other internet activity. The LIM Program consists of installing interception, monitoring and storage programs at international gateways, internet exchange hubs as well as ISP nodes across the country.

[24] Government of India, Ministry of Home Affairs, PRESS INFORMATION BUREAU, *Home Minister proposes radical restructuring of security architecture*, (December 23, 2009), http://www.pib.nic.in/newsite/erelease.aspx?relid=56395 .

[25] NATIONAL CRIME RECORDS BUREAU, Ministry of Home Affairs, http://ncrb.gov.in/BureauDivisions/CCTNS/cctns.htm (April 30, 2017).

[26] P. Chidambaram, Ex-Union Home Minister, *Ex-Union Home Minister's mission statement for NCRB under CCTNS*, CRIME AND CRIMINAL TRACKING NETWORK & SYSTEM (CCTNS), National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.nic.in/cctns.htm.

[27] Editorial, "India sets up elaborate system to tap phone calls, e-mail" The Reuters, June 20, 2013, 2:46 AM, http://www.reuters.com/article/2013/06/20/us-india-surveillance-idUSBRE95J05G2 0130620

These programs help the government have an unfettered access to petabytes of user data on a daily basis.

Network Traffic Analysis (NETRA) is real time surveillance software developed by the Centre for Artificial Intelligence and Robotics (CAIR) at the Defence Research and Development Organization (DRDO). It is used to detect voice traffic from Skype, Google Talk etc. as well as detection of real time keywords and key phrases such as bomb, blast, attack etc. on social media, blogs, tweets, emails and instant messaging services. It is mainly used for tackling crime and terrorism in India.

Indian Computer Emergency Response Team (CERT-In) has been established under § 70B of IT(Amendment) Act 2008 to serve as an agency to regulate the cyber space and provide for cyber security by

(a) collecting, analysing and disseminating information on cyber incidents
(b) forecasting cyber security incidents by making use of information available on cyber space
(c) handling cyber security incidents
(d) issuing guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

CERT-In has access to all the information available on cyberspace and the power to regulate the same.

Unique Identification Authority of India (UID scheme) or Aadhaar, currently referred to as a ticking time bomb, is a 12 digit unique-identity number issued to all Indian residents. It is based on their biometric and demographic data which is collected by the Unique Identification Authority of India (UIDAI), a statutory authority established under the Aadhaar Act 2016. It is the world's largest biometric ID system, with over 1.133 billion enrolled members as of 31 March 2017. The government by linking all the services with the UID number can easily monitor anyone continuously. [28]

Lastly, the National Counter Terrorism Centre (NCTC). The 26/11 attacks led to the genesis of NCTC. Based on the model of American NCTC and British Joint Terrorism Analysis Centre, the Indian NCTC, derives it powers from Unlawful Activities Prevention Act, 1967. However, the establishment of the NCTC would lead to concentration of powers pertaining to intelligence and operation, which would disrupt the autonomy of the states and would add to the bureaucratic tangle.

[28] Binoy Viswam v. Union of India, MANU/SC/0693/2017.

LEGISLATIONS SUPPORTING SURVEILLANCE

Erstwhile, the only substantive law supporting the state surveillance activities was the Indian Telegraph Act, 1855; however, with the technological boom and revolution, the Information Technology Act, 2000 was introduced to facilitate internet surveillance.

According to § 5(2) of the **Indian Telegraph Act, 1885**, "On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do 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, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

While § 5(2) forms the substantive part of the law, the procedure for the same is prescribed under **Rule 419A of the Indian Telegraph Rules, 1951**, introduced via amendment Act of 2007. As per this rule, the direction for interception, as specified in § 5(2) of the Indian Telegraph Act, can only be given by Union/ State Home Secretary. However, in unavoidable circumstances, a lawful order may be issued by, with the prior permission of the Union or State Home Secretary, an officer not below the rank of Joint Secretary to GoI. Pursuant to Rule 419A, service providers required by law enforcement to intercept communications are mandated to comply with certain provisions which include the appointment of nodal officers to deal with interception requests and to prevent its unauthorised usage. The licenses of the service providers stand to be revoked on non-compliance of these rules, resulting in breach of secrecy.

Sections 69 and 69B of **Information Technology Act, 2000** pertain to matters of web surveillance. § 69, is similar to § 5(2) of the Indian Telegraph Act, 1855. It provides for

interception, monitoring and decryption of computer sources by Central and State Governments in national interest. While § 69B, grants the Central Government the "power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security"[29].

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 lay down the procedure for invoking § 69 of the Information Technology Act, 2000 and is a replica of Rule 419A (as stated above).

Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 prescribe the procedure for invoking § 69B of the Information Technology Act, 2000 and is near- identical to rule 419A.

As per Rule 6 of **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,** a body corporate though disallowed from divesting information to a third party without the consent of the provider, may disclose the same without consent of the provider to the government agencies mandated under law for the purpose of verification, investigation etc.

Rule 3(7) of **Information Technology (Intermediaries Guidelines) Rules, 2011,** requires the ISP's etc., under a lawful order to provide authorized government agencies with information for identity verification etc.

As per Rule 7, **Information Technology (Guidelines for Cyber Cafe) Rules, 2011,** an officer may investigate the records of a cyber cafe and the owner has to comply with same and provide all the records, search history etc.

Aadhar Act, 2016 is one of the most controversial acts, it was passed by the Lok Sabha in March, 2016 to provide a legal backing to the UIDAI Scheme.

The government is in the process of developing rules for the compliance of § 67C of the IT Act, 2000, which may require the ISP's and Applications like Facebook etc. to store and collect data. For this purpose, the **Data Retention Rules Bill** has been drafted.

These rules put in place several checks and balances and try to ensure that there is an established "chain of custody" and paperwork for each and every detection and interception request. The assumption is that with a clearly defined chain of due diligence and paperwork, the possibility of unauthorized interception is

[29] Information Technology Act, 2000 (Act 21 of 2000), § 69B.

reduced, which ensures that the powers of the interception are not misused. However, although these checks and balances exist on paper, there is not enough information in the public domain about the whole mechanism of the interception for anyone to make a clear judgment as to whether the system in fact reduces the number of unauthorized interceptions.

INCIDENTS

Surveillance in India can be traced back to the A. K. Gopalan case, however, the issue of mass surveillance was raised in the "Telephone-tapping" case. Recently, apart from the WhatsApp and Aadhar card issue, surveillance reared its head in the **BBM case (2012)**.

Blackberry allowed the government agencies access to personal messages on the messenger post certain proposal from the Government of India. Next, in 2012, **The Hindu** released a report according to which several mobile phones were under scanner.[30]

Moreover in 2011, **Mr Milind Deora,** had (in Rajya Sabha) informed that the government had acquired technology to monitor contents on internet and had started surveillance on Facebook and Twitter.[31]

CONSTITUTIONALITY OF RIGHT OF SURVEILLANCE

Ever since their inception, the surveillance systems have had to navigate through muddy waters, with their constitutionality being questioned time and again. Various international statutes provide for the protection of rights and freedoms of citizens.

Article 19 of UDHR and ICCPR guarantee the right to freedom of opinion and expression. These articles hold that everybody has the right to hold opinions without interference and to obtain and convey information and ideas through any media, regardless of the boundaries. Unrestricted freedom of expression and expression, as provided by the UDHR and the ICCPR will be impossible if people have to live in constant fear of the sanction for their unpopular opinions or information, even in private forums. Furthermore, Articles 12 and 17 of the UDHR and the ICCPR guarantee the Right to Privacy. General Comment No. 16 (1988) by the Centre of Civil and Political Rights (CCPR) adopted by the United Nations Human Rights Council (CCPR) states that

[30] Editorial, *10000 phones and 1000 email Ids under scanner*, THE HINDU REPORT, (October 12, 2012), http://www.thehindu.com/news/national/10000-phones-1000-email-ids-under-the-scanner/article3992185.ece.

[31] Ranjit Sur, *People under surveillance, privacy law for whom?,* (November 5, 2012), http://sanhati.com/excerpted/5753/.

Surveillance, whether it was electronic or otherwise, interception of telephone, telegraphic and other communication forms, wire-tapping and recording of conversations, should be prohibited. The storage of information on computers, databases and other devices, whether by public bodies or individuals or corporations, must be regulated by law. No one should be subjected to arbitrary interference with privacy, family, home or correspondence or to attacks upon his honour or his prestige. Everyone has the right to the protection of the law against such interventions or attacks.[32]

Thus, the Indian Surveillance Systems must be formatted and reviewed, so that they are in conformity and in no in breach of these International Statutes and Standards.

In United States of America, the mass surveillance program of the National Security Agency (NSA) has been challenged as being unconstitutional by the American Union for Civil Liberties in the case of ACLU v. Clapper[33]. This is directly relevant to India, in view of our own Central Monitoring System (CMS) which goes much further. In addition to the submission of right to privacy, ACLU also argued that mass surveillance violated the freedom of association, implicitly mentioned in the American First Amendment and confirmed by a long series of cases. In India, this right is expressly guaranteed by the Constitution.

Alexander Abdo, Council for ACLU, stated in his arguments that "Imagine the government coming to your home every evening and forcing you to hand in all your calls for that day. Is not that a clear violation of *the Fourth and First Amendments?*" By repercussion, of course, this whole argument holds with the same force for Free Expression (Article 19 (1) (a)). There are, therefore, two questions which we must take into account: to what extent do Article 19 (1) (a) and Article 19 (1) (c) embody the Doctrine of the Chilling Effect; and what is the standard of security applicable according to Articles 19(2) and 19(4). There is a considerable amount of jurisprudence and precedents interpreting the "reasonable restrictions in the interests of sovereignty and integrity of India", and most of them point to a general proportionality test. However, the sheer scale and the degree of mass monitoring require a more precise examination.

Various countries across the globe have expressly recognised the right to privacy. The emergence of modern legislation in this area can be traced back to 1970. The first data protection law in the world was passed in the state of Hesse in Germany. This was followed by Sweden (1973), the United States (1974),

[32] UNIVERSAL DECLARATION OF HUMAN RIGHTS, (January 27, 1997), http://www.hrweb.org/legal/udhr.html.
[33] No. 13-3994 (S.D. New York December 28, 2013).

Germany (1977) and France (1978). Europe, in this crucial time developed two important instruments i.e. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[34]and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[35] which enunciated specific rules for the handling of electronic data. The rules in these two documents form the core of the data protection laws of dozens of countries. These rules describe personal data as data which seeks to provide protection at every step i.e. from collection till storage and dissemination. The right of a person to access and change their data is an essential part of these rules. With these instruments, European Union also enacted two directives which provide the citizens with wide range of rights and protections against misuse of their data. It also enunciates right to know where the data originated, right to have erroneous data rectified and right to withhold grant and permission to use the data in certain circumstances.

The crippled surveillance systems devised in India, not only violate human and fundamental rights, but also are an epitome of arbitrary use of power. §. 5 (2) of the Telegraph Act and §. 26 (2) of the Indian Post Office Act outline a two-stage examination before the tapping of telegraph or postal articles. The first stage consists of sine qua nons in the form of an "occurrence of the public emergency" or "in the interests of public security". The second set of requirements according to the provisions is "the interests of the sovereignty and integrity of India, the security of the state, the friendly relations with the foreign states or the public order or the prevention of incitement to commit a crime." The sections consider a legal fiction in which a public emergency exists and it is the interest of the sovereignty, the integrity, the security of the state or the maintenance of public order / friendly relations with foreign states. However, the term "public emergency" has not been clearly defined by the legislature or the courts. It, therefore, vests arbitrary powers in an official to order the interception of communication which violates fundamental rights. The Supreme Court in State of MP v. Baldeo Prasad[36] considered that a statute must not only provide adequate safeguards for the protection of innocent citizens, but also the administrative authority must be satisfied of the

[34] *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* Convention , ETS No. 108, Stasbourg, 1981.

[35] OECD, *Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data* , Paris, 1981

[36] AIR 1961 (SC) 293 (296).

existence of the (clearly laid down) prerequisites before issuing an order with respect to the same. If the statute failed to do so in respect to any condition precedent, then the law suffered from a weakness and was deprecated as invalid. [17] The question of the existence of the public emergency which is left to the sole determination of an administrative officer can be challenged on the ground of being arbitrary and in contravention to Article 14 of the Indian Constitution.

Moreover, Surveillance, as practiced in India, violates Article 19 of the Indian Constitution. The fundamental rights referred to in Article 19(1) cannot be shortened in any way outside the relevant provisions of Cls. 2-6.[37] The restrictive clauses in Cls. (2) - (6) of Article 19 are exhaustive and must be interpreted strictly.[38] And the same has been disregarded by those framing the surveillance legislations.

Though the Right of Surveillance of the State for national protection is not per se unconstitutional, but the arbitrary and unregulated use of this right is unconstitutional. The Indian Legislation, hence, suffer from various loopholes.

USE AND ABUSE OF SURVEILLANCE

The Central Monitoring System (CMS) was approved by the Cabinet Committee on Security (CCS) on 16 June 2011. Since then, the CMS has been operated by India's Telecom Enforcement Resource and Monitoring (TERM) cells and has been implemented by the Centre for Development of Telematics (C-DOT). The government uses surveillance for intelligence gathering, prevention of crime, the protection of a process, person, group or object, or the investigation of crime. Basically is it used to maintain national security and prevention of terrorism. But is it justified to do so while taking a toll on the fundamental and human rights of the citizens? Will it be justified if an unfettered power is given to the government officials without any responsibility and liability? Who will be held liable for any misuse of such arbitrary power? How will they be punished?

The existing Indian laws do not answer all these questions. The Central Monitoring System (CMS) was announced in 2011, but there was no public debate on it and the government has given little thought about how it will work or how it will ensure that the system will not be abused. The surveillance agencies have got unfettered access to all our personal data with no reliability for the misuse of the same. “No information has been made available about whose data will be collected, how the collected will be used, or how long the data will be

[37] Ghosh O.K. v. Joseph E.X. AIR 1963 SC 812; 1963 Supp. (1) SCR 789.
[38] Sakal Papers (P) Ltd. v. Union of India, AIR 1962 SC 305 (315); 1962 (3) SCR 842.

retained."[39] There is no statutory redressal mechanism in case of illegal interception and monitoring of information and communications by the State. These agencies are exempted from disclosing information about themselves as per §. 8 of the Right to Information Act, 2005 and hence operate without judicial or legislative purview. Moreover, these Surveillance programs are not in conformity with any of the 'International Principles on the Application of Human Rights to Communications Surveillance'. Hence, it is natural to presume that the Surveillance system might be abused. Its present vagueness and excessive control over communication can create a potential for unprecedented abuse. "CMS will involve an online system for filing and processing of all lawful interception requests, an electronic audit trail will be in place for each phone number put under surveillance."[40] It is still unclear that who will audit the audit trail? The same ministry which authorizes the surveillance requests? Moreover, the surveillance cameras in public places can be misused by officials who want to harass or blackmail their political enemies or opponents. And the lack of any privacy laws in India makes the systems more vulnerable to misuse.

Thus, what we have here is a country with an extremely high level of corruption, no data protection laws, no strict privacy policy and an unregulated monitoring system which lacks public and parliamentary debate prior to its implementation.[41] "If India doesn't want to look like an authoritarian regime, it needs to be transparent about who will be authorized to collect data, what data will be collected, how it will be used, and how the right to privacy will be protected,"[42] Hence, the introduction of privacy legislations is the need of the hour. A solid framework and proper legislations are also needed to give a legitimate backing and to control all the functions of the Surveillance systems in India so as to make sure that the power is not misused or used arbitrarily. The legislations need to entail laws on the repercussions of misuse of data, to ensure the protection of rights of citizens against illegal interception of calls and messages, a basic framework and guidelines for deciding whose conversations and activities will be intercepted and also making an independent body to audit the interception of data. Without these measures

[39] Stakeholder Report by the INTERNET DEMOCRACY PROJECT on *India's Universal Periodic Review: Third cycle*

[40] Editorial, *Govt tightens control for phone tapping*, TIMES OF INDIA, (Jun 18, 2013), http://timesofindia.indiatimes.com/india/Govt-tightens-control-for-phone-tapping/articleshow/20640273.cms?referral=PM.

[41] Maria Xynou, (January 30, 2014), https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

[42] Cynthia Wong, an Internet researcher at New York-based Human Rights Watch.

the abuse of power can't have sighted and rectified.

Thus, to secure the safety of the nation and to balance the same with the rights of the individuals in a democratic nation, a regulated use of surveillance needs to be encouraged while its abuse should be discouraged.

CONFLICT BETWEEN RIGHT TO PRIVACY AND SURVEILLANCE

The Surveillance programs of the Indian Government are having pejorative impact on the civil and fundamental rights of the people. The right to Privacy has been held to be a part and parcel of Article 21 and has now been acknowledged as a Fundamental Right flowing from Right to Life. The IT Act also provides for the right to privacy and data protection. Even though the security concerns of the Indian Government may be justified, the protection of data and privacy can't be ensured by the government with such flawed schemes having no framework, set rules and regulations, penal provisions or accountability for the same. Further, the UID Project as of now does not provide for any safeguards for the protection of privacy nor does it prescribe any obligations on the government agencies.

Talking about the conflict between the right to privacy and surveillance, the latter subjugates the civil and fundamental rights of the people, who are left with no remedies. This can be proved by the fact that India hitherto does not have any Privacy legislations and the only elderly Privacy Bill is yet to see the light of the day, accentuating the conflict between Right to Privacy and Surveillance.

It poses an even greater threat on the privacy of the citizens because, albeit the right to privacy has been held to be the part of Article 21, the citizens won't be able to enforce it because most of these surveillance agencies require the Network Operators, Internet Service Providers (ISPs) and Telecommunications Service Providers (TSPs) like Bharti Airtel, Jio, Idea and Vodafone to intercept the data and are the actual ones who invade our privacy, yet not falling within the definition of 'State' under Article 12.

It's not just India, but these fundamental right violations are carried out in most of the democratic countries in the name of national security and public emergency. US State Department in its annual review found out that there are about 90 countries which are engaged in illegally monitoring the communications of political opponents, human right workers, journalists and suspected people. This poses a threat to the rights of the innocent people, so much so that for example, in Japan, the police

were fined 2.5 million for illegally tapping the phones of the members of the Communist Party. Amidst the controversies like these in so many countries, there are countries who have successfully tackled this conflict. While dealing with the increasing surveillance practices, many countries have reacted by introducing specific rules governing the collection and handling of personal information. In these countries, the constitutional provisions pertaining to surveillance and privacy have been amended accordingly. One of the first legislations in this regard was passed in the Land of Hesse in Germany in 1970, followed by the laws in Sweden, 1973; USA, 1974; Germany, 1977 and France, 1978. The European Union had a major role to play in bringing about all these legislations which while protecting the rights of the people, ensure rightful surveillance for the purposes of maintaining national security. The 'Council of Europe's 1981 Convention for the Protection of Individuals' regarding the 'Automatic Processing of Personal Data' and the 'Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data' articulated the specific rules with respect to handling of electronic data. The rules have been given force by these two accords to ensure that the personal information gets protection at every step, from collection till its dissemination. The Conventions also allow the people to access and amend their personal data. These laws require the personal information to the obtained fairly and lawfully, and to be used only for the original specified purpose while making sure that the data collected is adequate, relevant and not excessive to purpose it is collected for. They also require the data to be accurate and up to date and most importantly ensure that it's destroyed after its purpose has been completed.
Thus, it is crystal clear that national security is a priority and must not be compromised due to the rights of few private individuals, however due consideration must be paid to the implications it has on the civil and fundamental rights of the innocent citizens.

IDENTIFICATION OF ISSUES AND RECOMMENDATIONS

The dispute over the existence of Right to Privacy in India and concerns over abuse of surveillance power by administrative authorities have existed since before independence. Thus, in order to protect the Indian democracy, to safeguard the fundamental rights and to exterminate threats to national peace and security and sovereignty, several changes need to be introduced. The recommendations are as follows:

1. **Comprehensive Privacy Legislation:** According to Article 21 no one can be deprived of their right to life except by the procedure established by law. Thus, the Indian Legislature should table, amend the Privacy Bills drafted in 2011, 2014 and 2016 to close all the loopholes and pass the same in order to provide the citizens of India with a cosmic privacy policy and to provide for a mechanism for the encroachment of privacy in certain cases.
2. **Justifiable reasons for impinging privacy:** While establishing a nexus between need and legitimate state aim and ensuring that means are proportional to object, the legislature should clearly lay down the justifiable reasons for infringing the Right to Privacy.
3. **§ 5(2) of Indian telegraph Act, 1855 and Sections 69 and 69B of Information Technology Act, 2000:** These sections support surveillance for protection of sovereignty, security of state, friendly relations, public order and prevention of offences, however, they fail to clearly define these terms. Hence, to prevent miscarriage of justice in the future, these sections should be amended and the explanations for the above mentioned terms should be incorporated.
4. **Rule 419A of the Indian Telegraph Rules, 1951:** The said rule refers to 'unavoidable circumstances' however, fails to offer an explanation of the same. Thus, this rule must be amended to explain the above phrase.
5. **Information Technology (Intermediaries Guidelines) Rules, 2011:** Rule 3(7) uses the terms 'lawful order' and 'request in writing' interchangeably, which leads to confusion and seemingly implies that a 'lawful order' as envisioned is a written letter from the government agencies and does not bear the force of law, thus inordinately simplifying the process and thereby, increasing the chances of abuse of power. Therefore, it is essential to amend this rule prevent the future abuse of this rule.
6. **Aadhar Act:** The Aadhar Act must be amended and provisions should be incorporated to safeguard the rights and information of the citizens, and to increase the confidence of the citizens in the scheme.
7. **Development of strong encryption and data protection system:** The executive should focus on the development of a strong encryption and data protection system to safeguard the personal data of

the citizens and to promote financial, medical, technical and generic privacy.

8. **Limiting discretionary powers of authority with respect to usage of personal data of individuals:** All the laws, as mentioned above, need to be amended to limit the discretionary powers of the concerned authorities with respect to the procurement and usage of personal data of the citizens.
9. **Enactment of statutes with respect to surveillance:** The confusion surrounding surveillance is leading to the development of fear amongst the citizens. Hence, statutes should be enacted to provide for Surveillance agencies by clearly stating their composition, duties and powers; also, the circumstances in which such surveillance may be permitted, and the procedure for surveillance must be codified. Provisions should be laid down to ensure accountability of surveillance agencies and officers and penalty should be imposed for abuse of power and for "failure to protect data"[43].
10. **Establish interface between the two rights:** Right to privacy and right of surveillance are two conflicting rights, yet, they need to coexist so that democracy can flourish and sovereignty and security of the nation can be maintained. Hence, the pillars of our democracy need to focus on paving a way for the coexistence of the two above stated rights by establishing interface between them.

CONCLUSION

After so many years and numerous judgments, Right to Privacy has been acknowledged. However, a clear picture is yet to emerge with respect to its extent. India is a democratic republic, and accordingly this right flows from the Constitution itself. Right to Privacy is not only implicit in but forms the backbone of Article 21. If there is no privacy, then how can personal liberty be recognized. Also, if there is no privacy then isn't the concept of life equivalent to mere animal existence? Thus, the Supreme Court while recognising privacy as a fundamental right held that pursuit of happiness is founded upon autonomy and dignity.

It is through brute force and guile, unrestricted surveillance ensures an omnipotent and omnipresent government that will have suspicion of its citizens as the default option, which is exactly how democracies come to an

[43] Information Technology Amendment Act, 2008 (No. 10 OF 2009), § 43A.

end – by giving the ruling oligarchy unbridled power to keep the citizens under watch so that they are rendered incapable of questioning them. Moreover, this is the age of information, wherein, information is power and internet is all pervasive. Thus, there are stark implications on the position of the individual where data is ubiquitous.

Thus, an interface needs to be established between the rights after clarifying their legal position, imposing limitations and reasonable restrictions on them.