Electronic Journal of Social and Strategic Studies Volume 5 Issue 1
Date of publication: 31 May 2024 Apr-May 2024
DOI: https://doi.org/10.47362/EJSSS.2024.5103

Government Surveillance against the right to privacy in matters of Cyberspace in India

Arghish Akolkar

Abstract:

With the advancement in technology in the 21st century, surveillance technology has also become highly pervasive, this has increased the debates surrounding the right to privacy and government-mandated surveillance. This research paper seeks to examine the nature of the Indian surveillance state in Cyberspace which is permissible under the laws passed by the legislature and the agreements that have to be signed by the telecom and internet service providers in line with the right to privacy which has been recognized by the honourable Supreme Court, also discussing the historical developments which have led to this right. Lastly, the paper also discusses the factors that are responsible for the continuance of the surveillance legislation in matters of cyberspace.

Keywords: Cyberspace, Government Surveillance, Right to Privacy in India, National security, Surveillance state, Data Privacy, targeted surveillance, Mass surveillance

Introduction:

The 21st century has revolutionised every aspect of human life, today we have access to information a few swipes and clicks away, twenty years ago this privilege would not have even been enjoyed by the most powerful men in Washington DC. This rapid democratisation of access to information, if looked at from a security perspective, has opened an unknown Pandora's Box, as we have seen increasing adaptation of cyberspace by various extremists and terrorists to spread their violent ideology easily into the minds of young and naive minds across the world. This nature of threat which arises from the increased access to such literature and subverted perspectives is one where once the action is committed it might be a bit too late, hence, necessitating an approach that seeks to pursue an active tracking and redressal of the spread of this literature continually. Hence culminating in the creation of an atmosphere of suspicion from the authorities, Francis Bacon[1] said in his essay on Suspicion[2] that the

[1] Francis Bacon (1561–1626) was one of the leading figures in natural philosophy and in the field of scientific methodology in the period of transition from the Renaissance to the early modern era. As a lawyer, member of Parliament, and Queen's Counsel, Bacon wrote on questions of law, state and religion, as well as on contemporary politics; but he also published texts in which he speculated on possible conceptions of society, and he pondered questions of ethics (*Essays*) even in his works on natural philosophy (*The Advancement of Learning*)

[2] Francis Bacon XXXI. Of Suspicion

DOI: https://doi.org/10.47362/EJSSS.2024.5103

> Idea of suspicions amongst thoughts are like bats among birds, they ever fly by twilight; certainly, they are to be repressed, or at the least well-guarded: for they cloud the wind; they leese friends; and they check with business, whereby business cannot go on currently and constantly

In the same essay, Francis Bacon had remarked on the effect of such suspicion:

> There is nothing makes a man suspect much, more than to know little; and therefore, men should remedy suspicion by procuring to know more and not to keep their suspicions in smother.

This understanding of suspicions, as presented by Francis Bacon through his essays, provides us an important insight when it comes to understanding the perennial need of Governments globally for surveillance in today's 21st century, where everyone has easily accessible radical and extremist literature, which further increases the range of the prospective radicals, with their being a highly suspicion based perspective towards anything which goes beyond the contours of normality as defined by the state, which like an ouroboros feeds on itself eternally.

In today's day and age, where everything has been going digital from ISIS actively seeking to radicalise disenfranchised youth across the globe to join their terrorist cause and then sharing various online toolkits that seek to teach the youth how to make a dirty bomb (cylinder bomb, cooker bomb, etc.) we have seen this in the case of Coimbatore bomb blast in 2022 (The Hindu, 2022), while at the same time, there have been various instances where the carte blanche powers of the government have been used to conduct surveillance on people who were on the wrong sides of the said government in power, now in the infamous Pegasus spyware case (The Hindu, 2023), or in cases where there is a complete misuse of the powers of the government for political ends, in the now infamous Niira Radia tapes controversy (Quint, 2023). Further, with the increased digitization of daily life, there has been increased argument in favour of expanding the rights and liberties of the citizens against the state in cyberspace as well, hence, these increased calls have led to growing recognition of the right to privacy and other adjunct rights, emerging from technology in the 21st century, across various democracies.

This paper will seek to examine the nature of the legal surveillance in India in the Cyberspace context with the right to privacy which has been recognised by the Supreme Court through Article 21 of the Indian constitution.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

What is Surveillance?

The term Surveillance over the years has had various meanings with there being a lack of a proper definition being provided for the same, especially in the context of 21st-century technology, which further muddies the water when it comes to having a well-defined definition for the term is the emergence of sousveillance (Thomson, 2020). The term surveillance has been broadly defined by Ross Bellaby as follows:

> Surveillance can cover a wide range of activities from CCTV cameras and'covertsurveillance' to dataveillance and datamining. Who the individual 'is', whe re s/he is going, with whom s/he is associating or what s/he is doing all become the concern of the watchful eye. (Bellaby, 2012)

At the same time, the various legislations in India that empower the government to conduct surveillance do not provide for a steadfast legal definition of the word surveillance. the Cornell law dictionary has defined the action of surveillance as follows:

> Surveillance is the act of observing another to gather evidence. Surveillance is one of the most common methods law enforcement officials use to investigate suspects and gather evidence. It can be accomplished with the knowledge of the person being surveilled (overt surveillance) or without (covert surveillance).
>
> Generally, surveillance is electronic or fixed. Electronic surveillance includes wiretapping, bugging, videotaping, geolocation tracking, data mining, social media mapping, and the monitoring of data and traffic on the internet. Fixed surveillance includes covert surveillance of individuals in person, also referred to as "stake-outs". (Cornell law dicitonary, 2023)

For this academic paper, emphasis will be laid strictly on covert electronic surveillance in the realm of cyberspace.

Nature of Surveillance in India The earliest surveillance legislation in India traces back to its pre-independence British legacy of the Telegraph Act of 1885 [3] and the Post Office Act of

[3] The **Indian Telegraph Act, 1885** is the enabling legislation in India which governs the use of wired and wireless telegraphy, telephones, teletype, radio communications and digital data communications. It gives the Government of India exclusive jurisdiction and privileges for establishing, maintaining, operating, licensing and oversight of all forms of wired and wireless communications within Indian territory. It also authorizes government law enforcement agencies to monitor/intercept communications and tap phone lines under conditions defined within the Indian Constitution. The act came into force on 1 October 1885. Since that time, numerous amendments have been passed to update the act to respond to changes in technology.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

1895[4] , with the former being associated with cyberspace surveillance and the latter being associated with offline surveillance.

Since Independence, the Indian legislatures have approved various acts that have bolstered the powers of the government to conduct cyberspace surveillance, with these said legislations being further empowered with certain rules being issued by the Department of Information Technology. The various legislations and rules in India permit surveillance to be done in India, in the cyberspace domain, are as follows:

1. The Indian Telegraph Act of 1885
2. Indian Telegraph Rules of 1951
3. Code of Criminal Procedure of 1973[5]
4. The Information Technology Act of 2000[6]
5. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
6. Digital Personal Data Protection Act of 2023[7]

It has to be further noted that surveillance legislation is not the only way in which the surveillance apparatus of the government in the cyberspace domain gets created, equal attention and credit have to be given to the agreements that are signed by the government with the

[4] **The Post Office Act, 1896** is the enabling legislation in India which governs the various post offices which have been set up across the country, along with that it also discusses various requirements and scrutiny which is to be faced by a courier or a letter sent through the Post Office. This act was passed during the British Raj and hence allowed for the authorities to go through the various mails which were being sent across the country. This Act will supposedly be repealed and replaced by the Post Office bill, 2023 which is as per the time of publication has been introduced to the Rajya Sabha.

[5] **The Code of Criminal Procedure (CrPC)** is a fundamental set of laws governing the administration of substantive criminal law in India. It contains all enforced Central and State Acts linked with subordinate data like Rules, Regulations, Notifications, Orders, Circulars, Ordinances, and Statutes. It went into effect on April 1, 1974.

[6] **The Information Technology Act, 2000** provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cyber-crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes arising from this new law.[2] The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

[7] **The Digital Personal Data Protection Act, 2023**, was introduced on 3 August 2023 and passed by the Lower House of the Parliament on 7 August 2023 and the Upper House of the Parliament on 9 August 2023. The Act aims to regulate the processing of digital personal data and respect individuals' right to protect their data while recognising the necessity of processing and using such data for lawful purposes. The Act lays down procedures to process personal data in a lawful manner and aims to establish a comprehensive legal framework to govern digital personal data protection in India.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Telephonic Service Providers[8] and Internet Service Providers[9] , further, also the UAS agreement which has to be signed compulsorily by both the TSPs and ISPs to have operation in India.

The major parameter in differentiating between the surveillance legislations and rules from the various agreements that have to be signed by the ISPs and TSPs with the Indian government is that the focus of the former is primarily on targeted surveillance, though few sections of the IT Act do deal with mass surveillance and encryption[10] When it comes to the latter, the focus of surveillance clauses present in the agreement is primarily on mass surveillance, encryption and data storage of the same.

Structure of the Targeted Surveillance in India

In the Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary in the year 2014, on request of the General Assembly in resolution 68/127, had submitted a report on 'The right to privacy in the digital age', in the said document the UN Special Rapporteur had defined targeted surveillance as:

> the nature of surveillance which depend[s] upon the existence of prior suspicion of the targeted individual or organisation (UNOHCHR, 2014)

When we seek to analyse the nature of the targeted surveillance clauses in various legislations, along with the agreements that allow the government to do so, which are present in India, for better understanding we can understand these powers of the central government by clubbing similar clauses together and classifying them based on the nature of power it provides the government:

1. Complete seizure of Devices
    I. section 3(1AA) had defined the nature of the telegraph in such a way that nearly all electronic devices that can be used for communications fall under the definition of 'telegraph' for the said act. Hence, section 5(1) of the same act

[8] Telephone Service Provider means the provider of the mobile phone connectivity services and Mobile Phone Number used by the Customer on their mobile phones
[9] An Internet Service Provider (ISP) is **a** company that provides customers with access to the internet and other related services.
[10] Encryption is the process of converting human-readable plaintext into incomprehensible text, also known as ciphertext, to ensure that sensitive data remains unreadable to unauthorized users. It involves taking readable data and altering it so that it appears random.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

then subsequently empowers the Central Government or State Government or any officers of the law who have been authorised by the Central or State government to seize the devices or 'take temporary possession of any established telegraph' until the public emergency exists. There has been subsequently no definition of public emergency provided in the said legislation or in any other legislation or in the constitution, the constitution strictly discusses national emergency state emergency and financial emergency.

2. Interception and detention of information

I. The sub section 2 of section 5 of the Telegraph Act empowers the Central Government, State Government or any officer authorised by the Central and State Government, if they are satisfied that it is necessary or expedient, may by order, direct any message or class of message to or from any person or class of persons either the one sending the message or receiving, deny transmission or detain the message or make the message be disclosed to the government making that order or to the officer in charge.

II. The Procedure for the utilisation of the powers mentioned in sub-section 2 of section 5 of the Telegraph Act is detailed in the Indian Telegraph Rules of 1951's Rule 149A. This rule begins by reducing the permitted authorities to use section 5.2 of the Telegraph Act to the following:

A. Central Government: Order by Ministry of Home Affairs
B. State Government: Secretary to the State Government in charge of the home department
C. In exceptional cases, it can be issued by an officer not below the rank of Joint Secretary, authorised by the Union Home Secretary or State Home Secretary

III. section 419 of the Indian Telegraph rules empowers the Telegraph authority to intercept any message, as they deem fit, to intercept any message which is transmitted through the telephone, for the said purpose of any violation of these orders for the maintenance of the said equipment. Though this section of the rule makes it seem to be banal, it is to be noted that this provision is

DOI: https://doi.org/10.47362/EJSSS.2024.5103

complemented by rule 169(4) of the same act, which states that the Telegraph department is bound to furnish any information that it possesses on the order of the court of law or other competent authorities, which is furthering the already existing section 7 of the same act which clearly states that the official duty of the telegraph department shall include ensuring secrecy unless that secrecy is against the direction of the competent authority. Lastly, there is no clear definition of exactly who is the said competent authority. It has to be noted though that the provisions of Rule 419 and sections of the Telegraph Act are subject to the procedural hurdles or restrictions that are mentioned in Rule 419A.

IV. Further, the Ministry of Communication and Information Technology's Department of Telecommunication mandates and provides the template of the contract which has to be signed between the Telephonic Service Providers and the vendors of equipment, products and services, for the service that is covered under the scope of Telecom License Agreement held by the TSP. This agreement template has the following sections present in it:

A. Section 7.1 of the agreement lays the responsibility on the vendor to ensure that the equipment which is being supplied has everything that is required for conducting Interception, Monitoring, Analysis, etc. for the use by Law Enforcement Agencies and then further providing the complete information to enable these features, there should be a test carried out on the operationalisation of this feature after the commissioning of the network.
(It has to be noted that the stated 'equipment' in this stated section refers to the Lawful Interception
B. The previous section is supplemented by section 5.2.f, which mandates the vendor to use all reasonable endeavours to ensure that no viruses or code or anything disrupts or corrupts or interferes with the mandated lawful interception.

The important aspect that has to be noted is that none of the above two mentioned sections requires the vendor to keep the TSP in the loop of the data collection which is being done through the mandated equipment, not only the second section dissuade the vendor from installing anything which

DOI: https://doi.org/10.47362/EJSSS.2024.5103

may in any way hamper the capacity of the government to intercept the communications. Lastly, it has to be further highlighted that these sections, as in the implementation of equipment that provides the government access to the information, have to be installed mandatorily, hence, the cost will be borne by the licensee and not the government. This agreement allows the government to conduct targeted telephonic interception and monitoring without keeping the telecom provider in the loop most of the time.

3. Compulsory submission of Information

I. Section 91 of the Criminal Procedure Code empowers the Court or any officer in charge of a police station to issue summons for the production of any documents or anything that is deemed to be necessary for the purpose of any investigation, inquiry, trial or other proceedings under this code. This section of the CrPC has been often weaponised by the police to seek information from intermediaries, or otherwise access stored data. This section is further corroborated by Rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which makes a corporate body disclose sensitive personal data or information to the government without the prior consent for prevention or investigation of an offence, etc.

II. Further, the IT Act section 29 allows for the controller to have access to any computer system, any apparatus data or any other material connected with such system, on the grounds of their being a violation or suspected violation of the IT Act.

III. Section 7 of the Digital Data Protection Act of 2023, empowers the state to make a said Data Fiduciary process the personal data of a data principal without their prior consent, section 6 of the said act deals with the question of consent of the data principal, to the government on the following grounds when it comes to non-civil and non-health reasons:

A. Performance of function of the State, by state or its agencies, which means for the implementation of the laws or in the interest of the sovereignty and integrity of India or the security of the state. (s.7.c.)

B. Fulfilling any obligation under any law in India (s.7.d.)
C. Compliance with a judgement or decree issued under any law in India (s.7.e)
D. Public safety during a natural disaster or breakdown of public order (s.7.h)

IV. Section 36 of the Digital Personal Data Protection Act of 2023 directly states that: The Central Government may, for this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

4. Compulsory decryption of information:

With the growing trends of there being encryption of information across the internet, especially on the communication platforms that are used for day-to-day communications. The power of decryption[11] holds massive power as it allows the government to force the said company or service provider to decrypt the information that it had previously assured its customer that it would be encrypted, a way of ensuring that there will be privacy and secrecy maintained.

I. The rule 3 & 5 of the Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009 empowers the said competent authorities to intercept, monitor or decrypt information which is generated from computer resources, which has been loosely defined to include nearly all electronic devices.
II. The rule 6 of the same rules empowers the state government and Union Territory administrations to interception or monitoring or decryption of information beyond their jurisdiction, after clearance from the secretary in charge of the home department.
III. Rule 17 of the rules empowers the government authorities to make the decryption key holders to disclose the said decryption keys or provide assistance, this rule makes the key holders beholden to provide the nodal officer

It has to be further also noted that when it comes to encryption the government under the IT rules allows for encryption up to 40 bits only when it comes to mass data and a

[11] The process of decryption has been defined by the Indian Government under the Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009 as follows: "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code or algorithm or a combination thereof;

DOI: https://doi.org/10.47362/EJSSS.2024.5103

greater level of encryption can only be done with the permission of the government authorities. The 40-bit level of encryption could be decrypted by a regular computer through brute force back in 2004 within two weeks (Mohanty, n.d.). Ergo, today we do not have a comprehensive encryption policy present, there was one issued in 2015 it was withdrawn within 2 days.

5. Clamp down on End-to-End Encryption(E2EE)

   The government had issued IT rules, in 2021 intending to regulate OTT platforms and intermediaries. Section 4(2) of these new requires the Social Media Intermediaries which are primarily message providers to be able to identify the 'first originator' of content on the platform. Further, section 4(4) requires the social media intermediaries to "endeavour to deploy technology-based measures, including automated tools or other mechanism to proactively identify".

   As per Ria Pfefferkon, a research scholar at the Stanford Internet Observatory, these provisions are incompatible with E2EE, she states that when certain communication platform intermediaries use E2EE the data gets translated to unrecognisable gibberish, hence, if the government enforces these provisions which enforce the tracing of the primary originator of any message it will effectively put an end to the E2EE for all communication platform to adhere to the IT rules, 2021 (Pfeffkeron, 2023).

6. Carte Blanche under the Information Technology Act

   The section 69 of the Information Technology, to put the final nail in the coffin, empowers the government to issue directions for interception or monitoring or decryption of any information through any computer source, further empowering the government to collect any information that may be present in a computer resource, may that information arise from being generated by the computer, transmitted by the computer or receiving the said information or storing the said information. This power is available to the Central Government or the State governments or any officer who is empowered by either of them. This section further goes on to create a liability for any person who might be in charge of the said computer, to give the said information at their peril.

When it comes to the interception of communication, it can be legally done by Central Government and State Government level Law Enforcement Agencies. The Central

agencies which are authorised to do interception are as follows: – (i) Intelligence Bureau (IB), (ii) Narcotics Control Bureau, (iii) Directorate of Enforcement, (iv) Central Board of Direct Taxes, (v) Directorate of Revenue Intelligence, (vi) Central Bureau of Investigation (CBI), (vii) National Investigation Agency, (viii) Research & Analysis Wing (R&AW), (ix) Directorate of Signal Intelligence, Ministry of Defence – for Jammu & Kashmir, North East & Assam Service Areas. In the case of State Law Enforcement Agencies, the Director General of Police for that State or the Commissioner of Police, Delhi for Delhi Metro City Service Area (Raghavan, 2014)

Structure of the Mass surveillance in India

In the Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary in the year 2014, on request of the General Assembly in resolution 68/127, had submitted a report on 'The right to privacy in the digital age', in the said document the UN Special Rapporteur had defined mass surveillance as:

> Mass surveillance, whereby means "when states with high levels of Internet penetration can gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites." In a system of "mass surveillance," the report explained, "all of this is possible without any prior suspicion related to a specific individual or organization. The communications of literally every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned." (UNOHCHR, 2014)

Hence, while understanding the term Mass Surveillance as provided by the United Nations document, we will have to remove what constitutes lateral surveillance[12] , hence, strictly focusing on the nature of mass surveillance which strictly deals with the Telephonic Service Providers, Internet Service Providers and others. When one seeks to understand the mass surveillance apparatus of India it will be very important to understand the institutions that have been created by the Indian government to do the said mass surveillance, the organisations that primarily deal with this are the Central Monitoring Scheme (CMS), National Traffic Analysis

[12] Lateral surveillance is the act of 'watching over', The surveillance takes place between individuals themselves, without the involvement of any organizational entity such as the government, making it more decentralized and balanced.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

(NETRA) and National Intelligence Grid (NATGRID) (CPIL & Anr v.s. Union of India and ors, 2020). Hence, these organisations and schemes are briefly summarised as follows:

1. Lawful Intercept and Monitoring Project (LIM)

   The Lawful Intercept and Monitoring System, which has been being operated by the Centre for Development of Telematic (C-DoT0 in the Ministry of Telecom from the year 2011, is innately a government mass surveillance program that does surveillance of internet traffic, communication, web searches and all other data which may emerge from the internet. The government can do it through the installation of compulsory hardware between the Internet Edge Router and the core network by all the ISPs at their own cost on behalf of the government, hence, allowing the government unfettered direct access to all the Internet traffic that may flow through a certain Internet Service Provider. This system provides the government with the ability to run word or phrase-based keyboard searches, allowing the government to even have targeted

2. Crime and Criminal Tracking Network and Systems (CCTNS)

   Crime and Criminal Tracking Network and Systems (CCTNS), began in 2009. It is a project that aims at interlinking all the police stations under a common application software for investigation, data analytics, research, policy-making and providing citizen services such as reporting and trafficking of complaints, and requests for antecedent verification by Police. This project is being implemented with a collaboration of the Central and State governments. (MHA , GOI, 2023)

3. Central Monitoring Scheme

   The Central Monitoring Scheme emerged in the backdrop of the barbaric 26/11 attack, 26.11.2009 The Press Information Bureau, Government of India pitched the Central Monitoring Scheme as a centralised system to monitor communications on mobile phones, landlines and internet traffic in the country, to strengthen the security environment in the country. As per the response given by the Minister of State in the Ministry of Home Affairs to the unstarred question no.1007 in 2013, the salient features of the CMS are as follows:

   a. Direct Electronic Provisioning of target number by a government agency without any manual intervention from Telecom Service Providers (TSPs) on a

DOI: https://doi.org/10.47362/EJSSS.2024.5103

secured network, thus enhancing the secrecy level and quick provisioning of the target.

b. Central and regional database which will help Central and State level Law Enforcement Agencies in Interception and Monitoring.
c. Analysis of Call Data Records (CDR) to help in establishing linkage between anti-social/anti-national elements.
d. Research and Development (R&D) in related fields for continuous up-gradation of the CMS.

This was prepared by Telecom Enforcement, Resource and Monitoring (TREM) along with the Centre for Development of Telematics (C-DoT). The organisations that have access to this scheme are the Research and Analysis Wing (R&AW), the Central Bureau of Investigation (CBI), the National Investigation Agency (NIA), the Central Board of Direct Taxes (CBDT), the Narcotics Control Bureau, and the Enforcement Directorate (ED) and the National Intelligence Agency (NIA).

4. Network Traffic Analysis (NETRA) Project

This project has been said to be developed by the Centre for Artificial (CAIR), which is a lab under the Defence Research and Development Organisation (DRDO). The primary goal of this project is to monitor internet traffic, especially with a focus on keyboards such as ‘attack’, ‘bomb’, etc. on social media, emails and blogs. This will work as a massive dragnet surveillance system which is designed to monitor the nation’s internet networks including voice over internet traffic passing through software programs.

5. National Intelligence Grid (NATGRID) Project

This is a major counter-terrorism initiative that seeks to integrate public and private surveillance mechanisms, with the primary goal of utilizing big data and advanced analytics to study and analyse huge amounts of data and metadata related to various agencies and ministries of the Indian government, which includes tax and data account details, credit card transactions, visa and immigration records and itineraries of rail and air travel. This initiative will result in real-time profiling of individuals through the collection, aggregation and analysis of metadata of individuals, which could reveal various kinds of information across various ministries and social media.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

6. Advanced Application for Social Media Analytics (AASMA)
   It is designed to collect live data of users from multiple social networks, do sentiment analysis on the content they post, track their location, and alert authorities accordingly. (Common Cause, 2023)

Therefore, while keeping these schemes and initiatives in mind, for greater understanding we can classify the powers of mass surveillance of the government as follows:

a) Unified License (UL)
   A Unified License agreement[13] was created to implement the goal of 'One Nation - One License'. This agreement has to be signed by the parties providing the following services:
   a) Unified License (All Services)
   b) Access Service (Service Area-wise)
   c) Internet Service (Category-A with All India jurisdiction)
   d) Internet Service (Category-B with jurisdiction in a Service Area)
   e) Internet Service (Category-C with jurisdiction in a Secondary Switching Area)
   f) National Long Distance (NLD) Service
   g) International Long Distance (ILD) Service
   h) Global Mobile Personal Communication by Satellite (GMPCS) Service
   i) Public Mobile Radio Trunking Service (PMRTS) Service
   j) Very Small Aperture Terminal (VSAT) Closed User Group (CUG) Service
   k) INSAT MSS-Reporting (MSS-R) Service
   l) Resale of International Private Leased Circuit (IPLC) Service

   This agreement contained the following provisions about the powers of the government to do surveillance:

[13] National Telecom Policy - 2012 recognizes that the evolution from analog to digital technology has facilitated the conversion of voice, data and video to the digital form. Increasingly, these are now being rendered through single networks bringing about a convergence in networks, services and also devices. Hence, it is now imperative to move towards convergence between various services, networks, platforms, technologies and overcome the existing segregation of licensing, registration and regulatory mechanisms in these areas to enhance affordability, increase access, delivery of multiple services and reduce cost.Further, it envisages providing secure, reliable, affordable and high quality converged telecommunication services anytime, anywhere for an accelerated inclusive socio-economic development. One of the objectives of the National Telecom policy-2012 is "Strive to create *One Nation - One License*" across services and service areas

DOI: https://doi.org/10.47362/EJSSS.2024.5103

A. Chapter IV, Para 23.2 of the UL: requires the said Licensee to provide the required interception equipment for each service that they provide, at their cost of installation and maintenance.
B. Chapter VI, Para 40.2 of the UL. The licensee must provide facilities whenever interception has to be carried out by the government.
C. Chapter V, Para 37.1 of the UL: The agreement forbids the licensee from engaging in bulk encryption, which falls beyond the preview of the maximum allowed encryption as per the Information Technology Act,2013.
D. Chapter VIII, Para 8.3 of the UL: The licensee is required to provide the detailed call records of specified calls if requested by the security agencies
E. Chapter VIII, Para 8.5 of the UL. The licensee is required to provide the location of the mobile customers, as required by the UL.
F. Chapter IX, Paras 7.1 to 7.3 of the UL The licensee is mandated to maintain the logs, for a minimum of a year, of the log-in and out activities of all users of the services that are provided by the licensee, which may include: mail, internet access, etc. They are also further required to maintain the records about the network address and IP address
G. Chapter IX, Paras 8.1 to 8.3 of the UL: Lawful Interception and Monitoring (LIM) systems are required to be set up by the licensee for the internet traffic, at their own cost of installation and maintenance, the LIM should be set up in a fashion that allows for the downstream ISP which passes through the licensee's network to be monitored.
H. Chapter XI, Para 6.6 of the UL. The State and Central Governments designated office holders enjoy the right to monitor the telecommunication traffic which is in every gateway/router or technically feasible point in the network set up by the licensee

b) Unified Access License Service Agreement (UAS)

The UAS[14] was amended back in 2013, the amended clauses provided an overarching power of the government to conduct mass surveillance under the now amended clause 41.10 of the said agreement, the provisions of this amended clause are as follows:

[14] Unified Access Service (UAS) License agreement, as defined by the Department of Telecommunications, is an agreement which is signed between the government and a said licensee for the goal of providing wireline as well as wireless service in a defined area

DOI: https://doi.org/10.47362/EJSSS.2024.5103

A. Licensees (Telephonic Service providers) are obligated to provide connectivity up to the nearest point of presence of the MPLS[15] (Multi-Protocol Label Switching) network to the Central monitoring system at their own cost in the form of dark fibre with redundancy.
B. The licensee is obligated to ensure that their suitable redundancy in the chain of the monitoring equipment for trouble-free operations of monitoring at least 480 simultaneous calls as per the requirements.
C. The licensee along with the monitored calls is obligated to share the records pertaining to the: called/calling party mobile numbers, time/date and duration of the interception, location of the person at the other end of the phone call along with their cell ID and time to time directions which can traced using Global Positioning System, data records of even the failed calls and finally also the Call Data Record of the roaming subscriber.

c) Information Technology Act's section 69 B

Under this provision, the government is empowered to monitor and collect traffic data or information through any computer resource for cyber security

As has been enumerated under the previous section, this provision of the Information Technology Act permeates a said government to gain access to any form of information that may arise from a said government, may this information be local or on the server or on the cloud. This section has been worded very liberally, allowing for their being a broad interpretation of what may constitute information arising from a computer resource, this nature of interpretation can be seen with the usage of internet filtering technology by the government, especially for social media websites.

d) Others

Rule 7 of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011, makes it mandatory for Cyber Cafes to provide every document and required data, including personal information and internet search history, to the officer on demand. Further, Rule

[15] Multi-Protocol Label Switching (MPLS) is an IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

5 of the said rules mandates that the Cyber Café must store the log register for 1-year minimum.

Statutory restrictions on the powers of government surveillance

The nature of statutory restrictions which are enforced on the surveillance powers of the government, depends from act to act:

1. Telegraph act,

   The power of surveillance mentioned under section 5 of the Telegraph Act is restricted by the same section 5.2 of the same act, which provides the following conditions which need to be met:

   - Grounds: public order and safety, occurrence of public emergency, interest of the sovereignty and integrity of India, security of the state, friendly relations with foreign states
   - Authorised personnel: Central Government, State Government, or any officer who is authorised by either the Central Government or State Government
   - Required documentation: the reason for the utilisation of the powers mentioned in this section requires the said authorised personnel to state the reasons in writing, by order, direct message to the Government when the said orders have been issued by the said personnel in emergencies

   Due to the innate overwhelming nature of the surveillance which is permitted under the ambit of this section, the Central Government provided for greater restrictions and conditions which have to be met when the government seeks to use the powers mentioned under section 5 of The Telegraph Act, 1885. They are mentioned under Rule 149A of the Indian Telegraph Rules, 1951 as follows:

   1. Orders under the section can only be issued by the Secretary for the Ministry of Home Affairs in the Central Government and the secretary in charge of the Home Department under the state government
   2. In cases where the permissions orders cannot be obtained, due to the presence of certain dire circumstances, the said dire circumstances include remote areas where there is in an issue of interception of messages or for operational reasons when obtaining the messages is not possible.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

3. Interception orders can only be carried out with the approval of the senior most officer of the law enforcement agency of the said, which is not below the rank of Inspector General of Police at the state level. When the interception confirmation isn't received within 7 days of the request, the request is to be considered to be rejected if prior approval of the Union Home secretary or State Home secretary is not received.
4. The interception order should contain the information all important information regarding the person or the class of people who are the target of such interception. Further, the order should also contain the name and designation of the officer who had recommended such an interception. Every interception order would be valid for 60 days unless granted an extension of up to one hundred and eighty days. Further, the interception order should be delivered in writing to an officer who isn't below the rank of Superintendent of Police or Additional Superintendent of Police or equal rank.
5. The information which is obtained in the given time frame through the interception order is to be properly recorded by the said officer in charge, further copies are to be also made. The date of destruction of such copies can only be decided by the interception order permitted.
6. The interception order by a requisitioning law agency has to be sent to two nodal officers, who are appointed by the said company, who should be part of the senior executives., these nodal officers shall receive the interception requests from each state / UT / Service area, after receiving such a request they are expected to send an acknowledgement within two hours on receipt of intimations of interceptions. In exceptional cases, acknowledgement can be granted without prior approval.
7. While the law agencies should also appoint nodal officers, who wouldn't be below the rank of Superintendent of Police or Additional Superintendent of Police or another equal rank, they will be responsible for authenticating and sending the requisition for an interception to the nodal officers of the said company, which is to be delivered to the officer, not below the rank of sub-inspector of police.
8. The nodal officers of the company are required to create a list every fifteen days of the list of authorisations for interceptions that were received by them. This list should include the details of the references and date of order of the Union

Home Secretary or State home ministry, the date and time of the receipt of such order and the date and time of the implementation of the said order. Further on, the said service-providing companies are also duty-bound to have their own set of internal regulations to prevent from their being mischief by their employees through such interception orders for their own personal reasons, if they fail to do so under the Telegraph Act, they will have their license revoked or suspended.

9. Every confirmation of the interception order has to be reviewed by a review committee, which is to be provided with a copy of the interception order, the reasons why such an order was sought and why normal means couldn't be used to obtain that said information. The review committee may be set up by the Central or State Government, depending upon the case. For the central government it should constitute:
    - Chairman: Cabinet Secretary
    - Members: Secretary to the Government of India in charge of Legal Affairs and Telecommunications

    In the case of the state government, it should include the following:

    - Chairman: Chief Secretary
    - Members: Secretary of Law / Legal remembrance in charge and Secretary to the State Government (other than the Home Secretary)
10. The review committee is required to meet once every two months and record their findings about an interception order that has been issued by the said government official, if the interception order is said to be in not accordance with the legal requirements, then the review committee may set aside such directions or orders for the destruction of the copies of the said intercepted message or class of messages.
11. The recordings about the interception order shall be destroyed by the relevant authorities every 6 months unless required to be kept. The service providers are also required to destroy the directions of the interception of the message within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

2. Information Technology Act

There are no inbuilt safeguards, present in the legislation itself, which restricts the usage of section 29 of the act which is empowered to seize electronic devices on grounds of a suspected breach of the law. The Information Technology Act does provide restrictions on the powers of section 69 of the same act, the carte blanche surveillance provision, the following conditions need to be met to use the powers provided in section 69 of the said act:

a) Grounds: sovereignty or integrity of India, defence of India, security of the state, friendly relations with a foreign country, public order, prevention of a cognizable crime and investigation of a crime
b) Empowered personnel: Central or State Government officers, any officer who is authorised by the Central and State Government
c) Paperwork: the reason for which this section has been operationalised has to be mentioned

However, in the case of section 69B of the IT Act, the following grounds are required to be fulfilled to operationalise the said section:

- Enhancing cyber security
- Identification, analysis and prevention of intrusion or spread of computer containment in the country

These grounds require the government to further use the provisions by issuing a notification through the official gazette. Hence, the *probleme principle* is the definition of the word cyber security, which is defined under section 2 of the IT Act as follows:

> ‘Cyber security’ means protecting information, equipment, devices computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Ergo, any measure that is defined by the government as seeking to enhance cyber security or dealing with a said computer containment country, can be held as a credible ground for permitting any agency to monitor and collect traffic data or information that is generated, transmitted, received or stored. With there being no subsequent ways in which the said decision on the grounds can be questioned or subsequently revised by the government.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

3. Digital Personal Data Protection Act

   Under this act, there exist two specific provisions that explicitly empower the government with surveillance powers, they are section 7, 17 and 36 of the said act primarily. The Data fiduciary is empowered, under the below-mentioned grounds, to process data for the State and any of its instrumentalities under the following grounds:

   - To provide or issue to the Data Principal such subsidy, benefit, service, certificate, license or permit as may be prescribed
   - Interest of the sovereignty and integrity of India or the security of the state
   - Fulfilling any obligation under any law which is in force in India on any person to disclose any information, subject to such provisions being in accordance with the provisions regarding the disclosure of such information in any other law in force
   - Compliance with any order or judgement issued under a law which is in force in India

   While in the case of section 17, sub clause 2 states that all the provisions of the said act regarding the processing of personal data when such is being notified by the instrumentality of the State as the Central Government may notify, on the following ground:

   - Sovereignty and integrity of India
   - Security of the state
   - Friendly relations with the states
   - Maintenance of public order
   - Preventing incitement to any cognizable offence

   For the purpose of processing, section 2 of the act has defined by Digital Personal Data Protection Act, 2022 has been defined as:

   > Processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Lastly in the case of section 36 of the said act, for the matters of this act, the government may require the board and Data fiduciary or intermediary to furnish such information as it may call for.

4. Structural Operating Procedure issued for the Lawful Interception of Communications The government has an established SOP/instructions when it comes to the processing, executing and conducting oversight of the interception of telephones. The rules are constituted by an inter-ministerial group which is headed by the Home Secretary to consider the issue related to consider issues relating to the institutional framework of government for interception of messages/tapping of telephones, email, etc. These guidelines are not to be made public by the government. (Ministry of Home Affairs, Government of India , 2012),

   As per the Hindu report, these guidelines are said to be surrounding the interception orders for the TSPs, which are now said to be required to provide for lawful interception and monitoring of telecom service providers.

Analysis of the Structural restrictions for surveillance

Even though various legislative restrictions are present in the legislation itself it has to be emphasized that there is a substantial amount of scepticism with which one has to approach the question of whether the due diligence[16] is being done by the state. The reason for the nature of scepticism towards the question of due diligence arises from the RTI which was filled inquiring into the number of interception orders which are sanctioned by the MHA through the review committee, the number back in 2013 was 7500 to 9000 orders for the interception of telephones and 300 to 500 orders for interception of emails (SFLC, 2014), with these amount of requests for interception being approved by a committee which holds its meetings once every month with a limited committee strength, prescribed to it under law, such healthy scepticism is warranted. It has to be further highlighted that the government is also known to violate the privacy safeguards, which they have introduced in the legislation, to monitor internet traffic (Hindu, 2023)

[16] Due Diligence has been defined by the Black Law dictionary as Such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the special case.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Evolution and Jurisprudence of the Right to Privacy in the Court of Law

> Individuals have a psychological need to preserve an intrusion-free zone for their personality and family and suffer anguish and stress when that zone is violated. Democratic societies must protect privacy as part of their facilitation of individual freedom, and offer some legal support for the individual choice as to what aspects of intimate personal life the citizen is prepared to share with others. This freedom in other words springs from the same source as freedom of expression: a liberty that enhances individual life in a democratic community (Geoffrey Robertson QC, 2007)

While seeking to highlight the importance of privacy in the 21st century Justice Kaul in the Puttuswamy Judgement had opined that:

> Privacy is also the key to freedom of thought. A person has a right to think. The thoughts are sometimes translated into speech but confined to the person to whom it is made. For example, one may want to criticise someone but not share the criticism with the world[17]

Further, the evolution of the right to privacy, especially in common law countries, can be seen in the landmark case of Campbell v MGN Ltd, in which Lord Nicholas had opined that:

> 12. The present case concerns one aspect of invasion of privacy: wrongful disclosure of private information. The case involves the familiar competition between freedom of expression and respect for an individual's privacy. Both are vitally important rights. Neither has precedence over the other. The importance of freedom of expression has been stressed often and eloquently, but the importance of privacy is less so. But it, too, lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual. And restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state[18]

The foundational debates for the right to privacy though primarily said to have emerged in India since the PUCL judgement by the honourable Supreme Court and then later substantially in the Puttuswamy judgement, it would be incorrect to not look into the debates that happened during the constituent assembly about this, under the aegis of right to property.

The discussion and deliberations that happened within the Advisory Committee on Fundamental Rights provide us with the required insight into the issue of the right to privacy,

[17] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. AIR 2017 SC 4161
[18] Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22

DOI: https://doi.org/10.47362/EJSSS.2024.5103

the moot issue of the deliberations surrounded the notes to the constituent assembly which were submitted by Sir B N Rau and K T Shah. These notes provided a broad overview of the constitutional rights that have been guaranteed across the different countries, further deliberating on the nature of balancing which is required between the 'dignitarian rights' and 'utilitarian development rights. Along with these notes, there were also additional notes that were submitted by Munshi and Dr Ambedkar, with the latter being sceptical of the private power. K.T Shah through his writings professed that the concept of privacy, or as he put it the 'privacy of the home', is an important aspect of civil rights and globally has been ensured under the right to liberty of person, with this note being supplemented by Dr Ambedkar in his States and Minority Report, where he mentioned that

> It is the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures

Even though, the right to privacy had never been mentioned in the constitution even after being mentioned under the umbrella of civil rights by K.T Shah, the discussions about the right to privacy during the constituent assembly were also discussed and mentioned in The Constitution of India Bill 1895 which recognised 'every citizen in his house an inviolable asylum', further being brought up under The Commonwealth of India Bill, 1925 and the Motilal Nehru report of 1928. Irrespective of the said attempts by the esteemed parliamentarians of the constituent assembly, the move to recognise the right to privacy as a right of its own was opposed by their colleagues of equally high repute, especially BN Rau and Alladi Krishnaswami Ayyar, on the ground of the said right restricting the civil litigation process along with curtailing the investigative powers of the police authorities, further, it was also argued that the said right would be disastrous because it would grant and elevate the status to every correspondence to that of state papers.

There were further three attempts made by Somnath Lahiri, Kazi Syed Karimuddin and Pandit Thakur das Bhargava. The most salient attempt was by Kazi Syed Karimuddin, where the importance of such provisions was recognised by Dr Ambedkar, even though the said addition of the aid provision was not voted on.

Right to Privacy in the Court of Law

The earliest question about the right to privacy in front of the Honourable Supreme Court emerged in the now landmark case of M.P Sharma v Satish Chandra, District Magistrate, Delhi

DOI: https://doi.org/10.47362/EJSSS.2024.5103

and Ors[19]. The primary issue in front of the honourable court in the said case was on the power of search and seizure which is enjoyed by the government against the erstwhile Article 19(1)(f) which dealt with the right to property. The Supreme Court in this case upheld the power of the Government to conduct search and seizure, stating that:

> A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to Constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right by some process of strained construction.[20]

This decision of the Honourable Court which upheld the right to search and seizure power of the government was reversed in the judgement which was delivered by the Honourable Supreme Court in the case of Kharak Singh v. State of Uttar Pradesh[21]. The Kharak Singh case revolved under the power of the Police, under the UP Police procedures, to conduct physical surveillance towards people who are to be 'historic sheeters', the surveillance may include entering the house of the sheeter, inquiring into his movements, and other such actions. In this case, the Honourable Supreme Court held that there was no issue with secretly entering the residence of the sheeter, as the right to movement is not affected and the person's right can't be affected if they aren't aware of an action happening, while the Court held any form of intrusion into the residence of the sheeter was a violation of personal liberty under the Article 21 of the Indian Constitution. The Supreme Court further elaborated its understanding of 'personal liberty' under article 21 of the Indian Constitution as follows:

> Is then the word "personal liberty" to be construed as excluding from its purview an invasion on the part of the police of the sanctity of a man's home and an intrusion into his personal security and his right to sleep which is the normal comfort and a dire necessity for human existence even as an animal? It might not be inappropriate to refer here to the words of the preamble to the Constitution that it is designed to "assure the dignity of the individual" and therefore of those cherished human value as the means of ensuring his full development and evolution. We are referring to these objectives of the framers merely to draw attention to the concepts underlying the constitution which

[19]M.P Sharma v Satish Chandra AIR 1954 SC 300
[20] M.P Sharma v Satish Chandra AIR 1954 SC 300
[21] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295

DOI: https://doi.org/10.47362/EJSSS.2024.5103

> would point to such vital words as "personal liberty" having to be construed in a reasonable manner and to be attributed that these which would promote and achieve those objectives and by no means to stretch the meaning of the phrase to square with any preconceived notions or doctrinaire constitutional theories.[22]

Even though the Kharak Singh judgement by the Honourable Supreme Court was considered a major step in the pursuit of the right to privacy, by having a liberal interpretation of 'Personal Liberty' mentioned in the article 21, the minority opinion was delivered by Hon'ble Subba Rao who went further than the majority opinion, which considered the right to secret entry in the absence of a person not a violation of the personal liberty of the individual under the article 21 of the Indian Constitution , her minority opinion recognised the right to privacy as an important facet of personal liberty under the article 21 by expanding on the understanding of personal liberty , provided by the Honourable Supreme Court in the A K Gopalan v State of Madras[23].

The Honourable Supreme Court in the case of R.M.Malkani v State of Maharashtra[24], when the question of admission of evidence was obtained from phone tapping, the court upheld the admissibility and also stated that:

> Article 21 was invoked by submitting that the privacy of the appellant's conversation was invaded. Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high-handed interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants. It must not be understood that the Courts will tolerate safeguards for the protection of the citizen to be imperilled by permitting the police to proceed by unlawful or irregular methods.[25]

The major landmark case about the question of the Right to Privacy was delivered by the Honourable Supreme Court in the case of Gobind v. State of Madhya Pradesh[26]. The primary issue surrounding the case was regarding the right of the police forces and the state apparatus to conduct surveillance in the private residence of a certain person. The Supreme Court in the said case held that these powers of the police were ultra vires to Article 21 of the Indian

[22] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295
[23] A K Gopalan v State of Madras AIR 1950 SC 27
[24] R. M. Malkani v State of Maharashtra 1973 AIR 157
[25] R. M. Malkani v State of Maharashtra 1973 AIR 157
[26] Gobind v. State of Madhya Pradesh AIR 1975 SC 1378

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Constitution, hence laying the foundation of the right to privacy in the country. The Honourable Court in the said case judgement stated that:

> 28. The right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right, we do not think that the right is absolute.[27]

This landmark case judgement was further supplemented by the Honourable Supreme Court in the case of R. Rajagopal v State of Tamil Nadu[28]. In the said case it was observed by the Honourable Court that:

> 26. We may now summarise the broad principles flowing from the above discussion: The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent — whether truthful or otherwise and 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 an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.[29]

The Right to Privacy was further cemented by the Honourable Supreme Court, in the case of People's Union for Civil Liberties (PUCL) v. Union of India[30], in which the Honourable Supreme Court clearly stated that:

> 17. We have, therefore, no hesitation in holding that the right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law.[31]

[27] Gobind v. State of Madhya Pradesh AIR 1975 SC 1378
[28] R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors AIR 1995 SC 264,
[29] R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors AIR 1995 SC 264,
[30] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301
[31] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301

DOI: https://doi.org/10.47362/EJSSS.2024.5103

The PUCL case was also further ground-breaking for the reason that in the case judgement, the honourable Supreme Court analysed the surveillance legislation that was currently present, especially analysing them in the context of the growing technological developments in the fields of surveillance. Given which the Honourable Supreme Court concluded that the provisions of the Telegraph are out of date, and weren't made in the times when the concepts of mass surveillance could be considered a possibility, unlike today. The Honourable Court also stated that there is a need for there being better safeguards, given the nature of the surveillance powers which are granted to the government by the statutes, especially to prevent any form of malafide actions or weaponisation of the said powers for narrow means. This case was considered to be a path-breaking judgement for the right to privacy and the powers of surveillance which are enjoyed by the government also because in this judgement the Supreme Court recognised the requirement for there being proper grounds and safeguards to ensure there is a right to privacy for the ordinary citizen in an ordinary setting.

The Honourable Supreme Court, in the case of K S Puttuswamy v. Union of India, a case in which the primary issue was the privacy concerns that arose from the Government's Aadhar Card Scheme as it sought to collect and compile data on demographics and biometrics of all Indian citizens. In the said case the Honourable Court held that with regard to the previous decisions of the court on matters of right to privacy:

> 821. The reference is disposed of in the following terms: i. The decision in M P Sharma which holds that the right to privacy is not protected by the Constitution stands over-ruled; ii. The decision in Kharak Singh to the extent that it holds that the right to privacy is not protected by the Constitution stands over-ruled; The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. iii. Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law.[32]

With Honourable Justice D Y Chandrachud holding that:

> 459. (A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality

[32] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. AIR 2017 SC 4161

DOI: https://doi.org/10.47362/EJSSS.2024.5103

between human beings and the quest for liberty are the foundational pillars of the Indian Constitution; …

(C) Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III; …

(F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognizes the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognizes the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being; …

Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the threefold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them; and Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.[33]

[33] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. AIR 2017 SC 4161

DOI: https://doi.org/10.47362/EJSSS.2024.5103

By way of this judgement, the honourable Supreme Court recognised the right to privacy to be an intrinsic right, which emerges from article 21 of the Indian Constitution, further also holding that the right to privacy is inseparable from a human element in human beings and core of human dignity, which has been defined and itself recognised as an intrinsic right from the Maneka Gandhi v. Union of India judgement[34]

Admissibility of evidence obtained illegally in the eyes of law

Section 5.12 of the Indian Evidence Act states that there needs to be a test of relevancy in the eyes of the law when it comes to the question of the admissibility of evidence which is obtained through illegal measures. The earliest case that dealt with the question of the admissibility of illegal evidence in the eyes of the law was the R M Malkani case[35] in which the honourable Supreme Court had held that the question of the admissibility of illegal evidence has to be decided by the respective judges on a case-by-case basis, deciding on the grounds of unfairness and self-incrimination. This precedent, with hindsight seeming to be antithetical to Article 21 of the Indian Constitution, was upheld in the subsequent cases by the honourable court such as in the case of the Pooran Mal case[36]. In the Pooran Mal case, the Honourable Supreme Court held that the question of admissibility of illegally obtained evidence can only be decided through a test of relevancy enshrined in section 5.12 of the Indian Evidence Act, the same was upheld by the Honourable Supreme Court in the Bharati Tamang Case[37].

The R M Malkani precedent was delivered by the honourable Supreme Court after the Kharak Singh judgement[38], in which the honourable court provided for a liberal interpretation of article 21 of the Indian Constitution while rejecting the concept of the right to privacy. The R M Makani judgement was further also not affected by the Maneka Gandhi judgement[39] which detailed the meaning of the ‘due process of law’, as was seen in the Bharati Tamang case.

The prior efforts of the Honourable Supreme Court led up to the Puttuswamy judgement in which the Honourable Supreme Court prescribed a three-pronged test on the question of such admissibility: just, fair and reasonableness. Since the introduction of the three-fold Puttuswamy judgement, the honourable high courts have restricted the powers of the government prosecutors to bring up evidence in various cases, which have been obtained from illegal

[34] Maneka Gandhi v. Union of India judgement AIR 1978 SC 597; (1978) 1 SCC 248
[35] R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471
[36] Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345
[37] Bharati Tamang v. Union of India, (2013) 15 SCC 578
[38] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295
[39] Maneka Gandhi v. Union of India judgement AIR 1978 SC 597; (1978) 1 SCC 248

DOI: https://doi.org/10.47362/EJSSS.2024.5103

means. The two prominent cases in which the Honourable High Courts rejected evidence on grounds of the Puttuswamy three-fold test are by the Delhi High Court in the Jatinder Pal Singh v CBI[40] and the Bombay High Court in the Vinit Kumar v CBI[41]. In the case of Vinit Kumar, the Honourable Court struck down the interception order as it went against the three-fold test prescribed under the Puttuswamy judgement and in the case of Jatinder Pal Singh, the Honourable Court held that on grounds of non-compliance with the three-fold test, there exist arbitrariness which is therefore violative of the right of the citizens, thus, the charges against the petitioner in the said case was dropped.

Limitations of the right to privacy under the Indian law

A. Public emergency as a ground for surveillance

For the application of section 5.2 of the Indian Telegraph Act, 1885, the precondition for its application is the requirement for their being a public emergency and the said thing being in the public interest. When understanding the required conditions, the condition of public interest has been further elaborated, the condition of public emergency is mentioned and not has been elaborated upon, neither in the legislation nor in the Constitution, which defines the conditions for National Emergency under the article 352, hence, making it a situation which if un-abetted provides the State with a carte blanche right to conduct surveillance under this section.

The Hon'ble Supreme Court, echoing the concerns of the 38th Law Commission Report on the Indian Post Office Act, stated that a proper definition is absent when it comes to the public emergency. It was highlighted by the Hon'ble Court in the case of the State of Madhya Pradesh v. Baldeo Prasad[42], it was stated that arising out of the public emergency conditionality clause in section 5.2 of the Telegraph Act, the conditional administrative authority had empowered the state to restrict the rights of a citizen then it reiterated the dissenting opinion of Lord Atkin in the case before the House of Lords in Liversidge v. Anderson[43] that in cases where the power which arises from a conditional clause with the conditions of which not being prescribed the said authority which is empowered by the said authority is said to enjoy absolute power, the

[40] Jatinder Pal Singh v. Central Bureau of Investigation, CRL. M.C. 3118/2012. (Order dated: January 17th, 2022)
[41] Vinit Kumar v CBI 2019 SCC OnLine Bom 315
[42] State of M.P. v. Baldeo Prasad, AIR 1961 (SC) 293 (296)
[43] Liversidge v. Anderson [1942] A.C. 206

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Honourable Justice Gajendragadkar further stated that in case of such provisions in any such act where the conditions haven't been prescribed then the said act is to be considered as *ultra vires* to the Indian Constitution.

B. Nature of the Right to Privacy in India against Government Surveillance

The Hon'ble Supreme Court in its landmark case of Puttuswamy v. Union of India[44] had held that while the right to privacy exists in India, emanating from article 21 of the Indian Constitution), the judgement reiterated the proportionality test which was given by the Honourable Supreme Court in the case of Modern Dental College & Research Centre[45] , which are as follows:

1. Measures restricting the right must have a legitimate state aim and be rationally connected with the aim (legitimate goal stage)

   Under this heading the primary words of focus are 'legitimate state aim', Justice Chandrachud has stated that:

   > The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits,

   The concept of 'the legitimate state aims' has been defined the order in a broad sense, with the key focus again in that said sentence being that of 'social welfare benefits', the definitions of which may vary from person to person or state to state. Hence, the honourable Justice to elaborate the point on social welfare benefits has stated that:

   > In a social welfare state, the government embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of

[44] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1, AIR 2017 SC 4161
[45] Modern Dental College and Research Centre & others V. State of Madhya Pradesh & others (2016) 7 SCC 353

> resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. However, the data that the state has collected has to be utilised for legitimate purposes of the state and ought not to be utilised unauthorizedly for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns.[46]

2. There must not be any less restrictive but equally effective alternative
3. The measure must not have a disproportionate impact on the right-holder

Though the aforementioned points from the previously referred judgement were reiterated in the Puttuswamy judgement, Justice Kaul in his judgement in this judgement had presented a very nuanced perspective on the understanding of 'invasion of privacy' stating that:

> The concept of "invasion of privacy" is not the early conventional thought process of "poking one's nose in another person's affairs". It is not so simplistic. In today's world, privacy is a limit on the Government's power as well as the power of private sector entities.[47]

Justice Kaul had stated in his judgement while reiterating the test which had been prescribed in the Modern College of Dentistry and Research Centre judgement[48], he had further stated the various other grounds on which the Right to Privacy of a said individual can be curtailed, are as follows:

a) Legitimate national security interest
b) Public interest includes scientific, historical or statistical purposes
c) Criminal offences
d) Anonymised data
e) Taxes

[46] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1, AIR 2017 SC 4161
[47] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1, AIR 2017 SC 4161
[48] Modern Dental College and Research Centre & others V. State of Madhya Pradesh & others (2016) 7 SCC 353

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Analysis of the right to Privacy with the Surveillance powers of the state and the Way ahead

The right to Privacy has substantially evolved over the years, with the earliest cases completely rejecting the notion of the right to privacy under Article 21 of the Indian constitution to the current precedent set under the Puttuswamy judgement in which the right to privacy was recognised as very integral to right to life and liberty under the article 21 of the Indian constitution. It has to be noted that the right to privacy in India, especially the judicial precedents, have not come to be originally on their own but have emerged in cases which in one way or another have the primary issue being the surveillance powers of the government enjoyed under a certain statute. Further, to look into the question of the right to privacy there have been two high-ranking committees which had been set up which are the Justice Shah Committee and Justice Srikrishna Committee, which have provided a detailed analysis of the nature of the right to privacy which is allowed in India further providing various policy suggestions which can be implemented in pursuit of the right to privacy in India

The evolution and the application of the right to privacy over the years has been an important one in preserving the fundamental rights of the citizens, in a rapidly digitizing world. The Right to Privacy, which is now recognised under the law cannot be breached until the said 3 conditions which have been established by the honourable court met. Many have argued that the right to privacy in India is not as broad as they are when compared to the democratic counterparts in Europe and the USA, these arguments and comparisons even though are not unfounded, they have to be considered far too utopian and not in touch with reality and the lived history of the Republic of India.

In the history of the Republic, there have been two substantial efforts at understanding, exploring and expanding the possible understanding of the right to privacy and the power of surveillance possessed by the state, the two committees that were set up are the: Justice AP Shah group of experts in 2012 and the Justice B.N. Srikrishna Committee in 2017. Justice AP Shah group of experts in 2012, they were set up to explore the privacy laws of the country. the Justice B.N. Srikrishna Committee in 2017, which was constituted under the Union Ministry of Electronics & Information Technology to suggest policy recommendations on data protection.

DOI: https://doi.org/10.47362/EJSSS.2024.5103

When discussing the right to privacy in India, the following factors have to be kept in mind, before seeking the imposition of a Western construct and understanding of the said concept and principle in a country with a different lived history:

1. High record of societal violence, social strife, armed insurgencies and terror across the modern history of the Republic of India

   The modern history of India has been marred with various tragic events of mass casualties and harm, these may be from riots that have happened across India on the lines of religion, caste, etc., and history of insurgencies across the country, with the situation being of such a nation that most states in India have witnessed an insurgency previously or currently are witnessing an armed insurgency. The already existing tragic accounts of human loss increased with the history of the terror that has been seen in India over the years.

   Given these historical and ongoing factors, there is a greater requirement for surveillance in India to ensure that the primary function of the state gets fulfilled which is ensuring and protecting the right to life of all citizens of the republic. The silver lining on this aspect is that as per the NCRB data which has been published there is an increasingly declining trend which is being noticed, of such tragic events taking place and the human casualties which arise from such events (Kapur, 2023), hence with this over a few years it can be successfully argued for a greater expansion of the right to privacy in India.

2. Overdependence of the Police on surveillance

   Over the years there have been increasing calls for law-and-order reforms in the country, especially police reforms (Singh, 2022). The police have been overburdened, with limited manpower present with them for conducting both policing and investigation of crimes, further for conducting the said work they are poorly trained and equipped to do the same. This leads to there being a greater reliance on surveillance powers provided under the statute, to meet the ends of justice and incriminate the accused in a said case, rather than doing the investigation work that might be required in other countries, these interception orders are usually outnumbered by the request to the access to the surveillance cameras which are installed in the public areas by the private individuals under the section 144 of the CrPC (Sharma, article 14, 2023).

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Hence, it has to be stated that without broad policing reforms in the country, which will ensure that there is a reduced reliance on the Police on surveillance interceptions, expanding the scope of the right to privacy would be broadly infeasible.

3. Lack of general public awareness

   There is a greater lack of awareness present in the larger masses about the right to privacy of the individual (Common Cause, 2023) , which is an important area that requires a greater awareness campaign to be done. This has to be done to create a greater democratic consensus when it comes to having greater stop-gap measures about surveillance powers of the government and having a greater right to privacy.

Conclusion

The meaning of surveillance has evolved rapidly in the 21st century. The rapid technological development across all fields has increased the capacity of governments, all over the globe, to do surveillance and infringe on their personal spaces. This paper seeks to ascertain the contours of the Indian surveillance state in cyberspace, arising from various statutes and licensing agreements, while also understanding the legal restrictions, either arising through the statute itself or through judicial precedent, which are in a place to restrict arbitrary usage of these powers against an ordinary citizen. The primary statutes and ancillary rules which have been analysed are the Indian Telegraph Act of 1885, the Indian Telegraph Rules of 1951, the Code of Criminal Procedure of 1973, the Information Technology Act of 2000, The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and the Digital Personal Data Protection Act of 2023. The licensing agreements which have been analysed are the Unified License Agreement and Unified Access License Service Agreement. For greater clarity, the powers that arise from the said Statute, licenses and agreements have been classified into targeted and Mass surveillance powers of the state.

When seeking to understand, the nature of the rights which are enjoyed by the citizens which protects them from the previously mentioned powers of the state the rights are safeguarded by what can be called as the Statutory barrier and the Judicial barrier. The Statutory barrier refers to the statutory restrictions which are in place through the said legislation, which gives rise to the surveillance powers of the state, or ancillary rules which have been introduced by the

DOI: https://doi.org/10.47362/EJSSS.2024.5103

Department of Information and Technology subsequently or other related ministry. The Judicial barrier refers to the restrictions that have arisen through the decades of judicial evolution in the honourable Supreme Court, this judicial barrier has been analysed chronologically, to provide a sequential understanding of how the idea of the right to privacy has evolved against the surveillance powers of the government. Further, given the legal history of India of there being flouting of already set precedents, recent case laws where evidence which arose illegal surveillance was used, with illegal evidence referring to evidence obtained by infringing the aforementioned legal or statutory barrier, in the said cases irrespective of the said evidence being a relevant fact the cases have been dismissed.

While analysing the surveillance powers of the government and the right to privacy which has evolved, the Justice Shah committee and the Justice Srikrishna committee have been briefly discussed. The analysis further also lays down certain factors, in the context of the surveillance and right-to-privacy debate, which have to be understood before constructing an understanding of the narrow balancing action between the two, these factors include social strife, the nature of policing and the nature of public awareness. After analysis, of the cases and the said committees, the previously mentioned factors or ground realities have to be increasingly looked into while navigating the path between the government's right to surveillance, on grounds of collective security, and the right to privacy and liberty of an individual.

Acknowledgement

Author wishes to acknowledge the mentorship and guidance provided for this research by Dr. R Srinivasan, Dr. Ashok Dua and Cmde SL Deshmukh NM during his internship with DRaS-Praghna Research Writing Program.

References

Bellaby, R. (2012). What's the Harm? The Ethics of Intelligence Collection. *Intelligence and National Security* , 93-117.

Common Cause, l. N. (2023). *Status of Policing in India report 2023.* Common Cause and Lok Niti.

Cornell law dicitonary. (2023, October 27). *cornell law*. Retrieved from cornell law : https://www.law.cornell.edu/wex/surveillance

CPIL & Anr v.s. Union of India and ors, Writ Petition (Civil) No. 8998 of 2020 (P.I.L) (Delhi High Court December 2, 2020).

Hindu, T. (2013). *https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece*. Retrieved from the Hindu: https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

Kapur, A. A. (2023). *Internal Security in India: Violence, Order, and the State.* Oxford University Press.

Ministry of Home Affairs . (n.d.). *mha,gov.in.* Retrieved from mha,gov.in: https://www.mha.gov.in/en/divisionofmha/women-safety-division/cctns

Ministry of Home Affairs . (n.d.). *mha.gov.in.* Retrieved from mha.

Ministry of Home Affairs, Government of India . (2012). *Revised SOP issued for Lawful Interception of Communication.* New Delhi : Press Information Bureau .

Mr. M. K. Raghavan, M. f. (2014). MHA to Lok Sabha starred question 294. *Lok Sabha* . Delhi : Lok Sabha .

Pfeffkeron, R. (2021, March 3). *brookings.edu*. Retrieved from brookings : https://www.brookings.edu/articles/new-intermediary-rules-jeopardize-the-security-of-indian-internet-users/

Quint, T. (2023, october 27). *The Quint* . Retrieved from thequint.com: https://www.thequint.com/explainers/what-are-niira-radia-tapes-explained#read-more

rights, A. r. (2014). *The right to privacy in the digital age.* New York : Human Rights Council.

SFLC. (2014). *India's Surveillance State.* Delhi.

Sharma, B. (2023, November 24). *article 14*. Retrieved from article14.com: https://article-14.com/post/how-the-state-is-using-section-144-private-citizens-for-warrantless-surveillance--656010262fb8f

Singh, P. (2022). *The Struggle For Police Reforms In India: Ruler's Police To People's Police.* Rupa Publications .

The Hindu . (2022). *thehindu.com*. Retrieved from thehindu.com : https://www.thehindu.com/news/national/explained-the-operations-of-the-pegasus-spyware/article38352757.ece

The Hindu. (2022). *In coimbatore a bomb on wheels.* Coimbatore : The Hindu .

Thomson, F. K. (2020). The concepts of surveillance and sousveillance - a critical analysis. *Social Science Information*, 11.