OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 13, Nº. 2 (November 2022-April 2023)

JANUS.NET
e-journal of International Relations

PRIVACY AND SURVEILLANCE CONFLICT: A COMPARATIVE ANALYSIS OF THE LAWS IN THE USA AND INDIA

VAIBHAV CHADHA
vchadha@jgu.edu.in
Assistant Professor of Law at Jindal Global Law School, O.P. Jindal Global University (India). He holds a master's degree in law from Queen Mary University of London on a Chevening Scholarship. Vaibhav also has a bachelor's degree in law as well as commerce from the University of Delhi and a diploma in International Law and Diplomacy from Indian Society of International Law. In the past he has written international articles on anticipatory bail law in India, copyright law, freedom of speech and expression, privacy and surveillance, and on laws enacted to curb the practice of child marriage. Before moving to academia, Vaibhav worked at the Office of Advocate General of State of Nagaland, India, and Additional Solicitor General of India. His areas of interest include free speech, media law, and criminal law.

THAJASWINI COIMBATORE BALASUBRAMANIAN
thajaswini.cb@gmail.com
A qualified lawyer, who is currently pursuing her Masters of Law at the University of Cambridge. She holds a Bachelor of Arts and a Bachelor of Law (BA.,LLB (Hons.)) degree from the School of Law, SASTRA Deemed University (India). She was assisting a Senior Advocate at the Hon'ble Supreme Court of India for over a year, before pursuing her Masters. She is keenly interested in subject matters like Constitutional Law, Public Law, Commercial Taxation, Intellectual Property and Privacy Laws.

ANSHUL BHUWALKA
anshul.bhuwalka@induslaw.com
Associate (Transactions), IndusLaw, Mumbai, India. He holds a bachelor's degree in Law as well as Business Administration from Symbiosis Law School, Hyderabad (India) - Symbiosis International (Deemed University). He has written articles on constitutional law and contractual law, with specific reference to the corporate domain. His areas of interest are constitutional law, corporate and commercial laws

Abstract

The Right to Privacy and the need for Surveillance has always remained a contentious issue between citizens and law enforcement agencies. This paper attempts to analyse the various laws relating to Surveillance in the largest and oldest democracies of the world, India and the United States of America. Regardless of vast variances in socio-economic and political realities, these two countries qualify as intriguing focuses for study. Though the Right to Privacy is generally accepted as a fundamental right throughout the nations of the world, the primacy given to 'National Security' and simultaneously balancing it with individual liberties seems to be a recognised phenomenon in both these jurisdictions.

Keywords

Privacy; Surveillance; Unlawful Activities (Prevention) Act 1967; National Security; Kharak Singh v. State of Uttar Pradesh; Telegraph Act; Terrorism and PATRIOT Act.

Resumo

O Direito à Privacidade e a necessidade de Vigilância têm permanecido sempre como uma questão controversa entre os cidadãos e as agências de aplicação da lei. Este documento tenta analisar as várias leis relativas à Vigilância nas maiores e mais antigas democracias do mundo, a Índia e os Estados Unidos da América. Independentemente das grandes variações nas realidades socioeconómicas e políticas, estes dois países qualificam-se como intrigantes focos de estudo. Embora o Direito à Privacidade seja geralmente aceite como um direito fundamental em todas as nações do mundo, a primazia dada à "Segurança Nacional" e,

simultaneamente, o seu equilíbrio com as liberdades individuais, parece ser um fenómeno reconhecido em ambas as jurisdições.

Palavras-chave

Privacidade; Vigilância; Lei das Actividades Ilícitas (Prevenção) de 1967; Segurança Nacional; Kharak Singh v. Estado de Uttar Pradesh; Lei do Telégrafo; Lei do Terrorismo e Lei PATRIOT.

How to cite this article

Chadha, Vaibhav; Balasubramanian, Thajaswini Coimbatore; Bhuwalka, Anshul (2022). Privacy and Surveillance Conflict: A Comparative Analysis of the laws in the USA and India. *Janus.net, e-journal of international relations*, Vol13 N2, November 2022-April 2023. Consulted [online] in date of last visit, https://doi.org/10.26619/1647-7251.13.2.8

Article received on 17 April 2021, accepted for publication on 6 October 2022

JANUS.NET, e-journal of International Relations
e-ISSN: 1647-7251
Vol. 13, Nº. 2 (November 2022-April 2023), pp. 201-219
Privacy and surveillance conflict: a comparative analysis of the laws in the USA and India
Vaibhav Chadha, Thajaswini Coimbatore Balasubramanian, Anshul Bhuwalka

PRIVACY AND SURVEILLANCE CONFLICT: A COMPARATIVE ANALYSIS OF THE LAWS IN THE USA AND INDIA

VAIBHAV CHADHA

THAJASWINI COIMBATORE BALASUBRAMANIAN

ANSHUL BHUWALKA

1. Introduction and Background

"States are utilizing technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns".[1]

Surveillance typically means to closely observe an individual or a group of individuals, especially ones who are suspected by law enforcement agencies.[2] Currently, there exist various types of mechanisms for the government for surveillance. An efficacious government surveillance regime necessitates the assortment and handling of large scale personal data which includes sensitive and crucial information as well. Such laws and programmes raise vital concerns relating to data protection and privacy of millions of citizens which would be at stake. An effective government policy is one which efficiently lays a foundational balance between National Security through strategic surveillance and individual and collective privacy without compromising the rights Constitution provides. While the United States of America considers Electronic Surveillance as search under the Fourth Amendment which provides protection to individuals from unreasonable search and seizure, in India, it is still a growing concern.[3]

It is seen that majority of the people do not deter surveillance, stating they do not particularly have anything to hide. It is the very ideology behind this argument that is typically flawed, considering there is no rational assessment of how surveillance influences the behavior of a human. It is due to this that the "chilling effect" is induced, which makes people behave differently due to the apprehension of being watched, intercepted, or surveilled in any other way.[4] The chilling effect is said to occur when people seek to engage in activities that are well within their rights but are deterred due

1 *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Others* [2017] 10 SCC 1 503, [585]
2 SAHRDC, 'Architecture of Surveillance' [2014] 49 EPW 10, 12
3 Chinmayi Arun, 'Paper-thin Safeguards and Mass Surveillance in India' [2014] 26 NLSIR 105, 114
4 *Solove, Daniel J, 'The First Amendment as Criminal Procedure' [2007] 82 NYU L Rev 112, 154–59*

to governmental restrictions.[5] Therefore, surveillance directly affects an individuals' rights of essential liberties, like their right to privacy and freedom of speech or expression. Surveillance by the government can lead to curbing legitimate activities and restrain disagreement.[6] Concerns like these tend to startle public peace and must not be allowed in a country like India, which has vibrant democratic ethos.

2. Existing Surveillance Laws in India

One of the gravest breaches and threats to one's right to privacy is by having an individual surveilled. This surveillance can be of different forms, involving physical surveillance, telephonic surveillance, digital surveillance, or any other way to know everything about a person. As correctly pointed out by George Orwell, it leads to situation where the mere fact that an individual is aware of their activities being surveilled by another would cause them to change their conduct.

The two main laws that govern and regulate digital and telephonic surveillance in India are the Indian Telegraph Act, 1885 and the Information Technology Act, 2000. The Indian Telegraph Act, 1885 deals with interception of calls wherein under section 5, the act empowers the Central or the State government to order for interception of messages in case of occurrence of any public emergency or in the interest of public safety. Rule 419 B was included to the Indian Telegraph Rules, 1951 in the year 2007 which authorised an officer (not below the rank of a Joint Secretary to the Government of India) to pass an order for interception in unavoidable circumstances.

The interception of data is dealt with in the Information Technology Act, 2000. Section 69 of the Act empowers the government to intercept, monitor or decrypt any data or information stored on any computer resources for the reason of public safety, public order etc. The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules framed under section 69 of the Act in 2009 explicitly states that only the competent authority can issue an order for interception, monitoring or decryption of any information generated, transmitted, received, or stored in any computer resource which include mobile phones as well.

Section 69A of the Act provides the authority to the government to issue directions to block public access of any information through a computer resource. Section 69B gives the Central government the power to monitor and collect traffic information or data through any resource from the computer.[7] One of the noteworthy amendments to the Information Technology (Amendment) Act, 2008 was the removal of the preconditions of "public emergency" and "public safety" which are laid down in the Indian Telegraph Act, 1885, and extended the Government's power to order the interception of communications for the "investigation of any offense".[8] The Information Technology (Procedures and Safeguards for blocking for access of Information by Public) Rules 2009 prohibits

[5] Frederick Schauer, 'Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"' [1978] 58 BU L Rev 693
[6] Solove, Daniel J, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 44 SD L Rev 771
[7] Ashok Kumar Kasaudhan, 'Surveillance and right to privacy: Issues and challenges' [2017] 3 IJL 73, 81
[8] The Information Technology (Amendment) Act 2008

interception or monitoring or decryption of information without authorisation. However, under both these laws, only the government is authorized to conduct surveillance.[9]

Apart from the above major laws on surveillance, there are other statutes which provides for interception of communication and lays grounds upon their usage. The Unlawful Activities Prevention Act, 1967 (UAPA),[10] the prominent anti-terror law in India, proved to be a departure from some of the traditional criminal justice administration system and allowed legally intercepted information as an admissible evidence for an offence under the Act.[11] The Act has tried to strengthen anti-terrorism measures by redefining the term 'Terrorism Act' and providing stringent punishments for the same under sections 15 to18. The Act also conferred special powers for arrest, search, and seizure under sections 43A to 43D.

Section 26 of the Indian Post Office Act, 1898 also authorises the Central and State government to intercept postal articles in case of public emergency or for the interest of public tranquillity; Section 91 of the Indian Code of Criminal Procedure, 1973 monitors targeted access to stored data and information. Under rule 4(2) of the Information Technology Guidelines for Cyber Cafes Rules 2011, cyber cafes are required to retain copies of user identification for a period of one year and rule 5 mandates that the cyber cafes must retain logs of user information and browsing history for a period of one year.

The Personal Data Protection Bill 2019,[12] (PDP Bill) which was introduced in the Lok Sabha on 11th of December 2019 aims at striking a reasonable balance between security and privacy. Section 35 of the PDP Bill assures for an exemption for carrying out surveillance activities by government agencies for the reasons of national security, public order, friendly relations with foreign states, integrity and sovereignty, and for preventing any cognizable criminal offences.[13]

2.1. Analysis of the Indian Laws

Although it has been established that the authority to intercept a telephonic communication is provided under Section 5 of the Telegraph Act, in pursuance to the prescribed procedure, Rule 419A of the Telegraph Rules, 1951 restricts such authority to the Union Home Secretary in case of the Central law enforcement agencies, and the Home Secretary to the State Government, in case of the State law enforcement agencies. However, in unavoidable circumstances, the concerned law enforcement agencies with the permission of its head or the second highest ranking officer who is not below the rank of an Inspector General are permitted to carry out emergency interception. In such cases,

[9] Maria Xynou, 'Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles' [2015] CIS <https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf> accessed 06 March 2021

[10] The Unlawful Activities (Prevention) Act 1967

[11] The Unlawful Activities (Prevention) Act 1967, s 46

[12] Personal Data Protection Bill 2019

[13] Kazim Rizvi, 'Personal Data Protection Bill 2019 and Surveillance: Balancing Security and Privacy', [2020] INC42 <https://inc42.com/resources/personal-data-protection-bill-2019-and-surveillance-balancing-security-and-privacy/> accessed 06 March 2021

the said law enforcement agencies are bound to notify the Home Secretary in not more than three days to explain their quick action.[14]

Considering possible loopholes in the procedure, which may lead to breaching multiple fundamental rights of another, the Telegraph Rules 1951 also prescribe for a review mechanism[15]. The said review committee is headed by the Cabinet Secretary, Law Secretary, and the Secretary Telecommunications in case of Central law enforcement agencies and the Chief Secretary, Law Secretary, and another member other than the Home Secretary, appointed by the State Government in case of the State law enforcement agencies[16]. This committee is entrusted to review the copies of every authorisation of interception as received from the concerned Home Secretary within seven days. In case the review committee finds any authorization unreasonable or wanting, the respective interception is to cease with immediate effect.

On the face of it, these Rules followed by the stringent laws and protections seem comprehensive, having sufficient safeguards. However, on the basis of the Central government's response to various Right to Information (RTI) applications dated back in 2014, the Union Home Ministry annually approves about one lakh (one hundred thousand) requests of interceptions of telecommunications.[17] In this case, if we were to assume an average of about 8,000 requests per month, it would sum up to over 250 requests per day. It is important to note that while considering and reviewing such requests by the law enforcement agencies, the respective authority is to lay emphasis on a possibility to acquire the said information by alternate means, and if not, only then the reasons for such interception shall be recorded in the Order allowing it.[18]

It is apparent that law contemplates a quasi-judicial application of mind while deciding the request of interception and surveillance, and not a mere clerical process of ambiguously rejecting or approving such requests. It is however pertinent to note that the matters allowing jurisdiction to the Union Home Ministry include internal security, border management, affairs pertaining to Jammu and Kashmir and Ladakh, administration of union territories, Centre-State relations, national language, police, human rights, prison management and pensions.[19] However, it is far from imagination as to how one can do justice to all applications requesting to infringe the citizens' essential fundamental rights, considering the large number of such applications along with the variety of affairs of the Home Secretary, on an everyday basis. Furthermore, the fact that how many Home Secretaries have previously had technical competence or legal training to make such important decisions, has also been neglected.

Home Secretaries for the Union and the State are selected from the Indian Administrative Service. Although the extreme intelligence and the level of intellectual experience in

[14] Stakeholder Report, 'The Right to Privacy in India' [2016] UPR CIS India and Privacy International, <https://www.upr-info.org/sites/default/files/document/india/session_27_-_may_2017/js35_upr27_ind_e_main.pdf> accessed 08 March 2021

[15] Indian Telegraph Rules 1951, Rule 419A

[16] Indian Telegraph Rules 1951, Rule 419A (16)

[17] Zubin Dash, 'Do Our Wiretapping Laws Adequately Protect the Right to Privacy?' [2018] 53(6) E&PW <https://www.epw.in/engage/article/can-government-continue-unhindered-wiretapping-without-flouting-right-privacy> accessed 06 October 2020> accessed 16 February 2021

[18] SFLC, 'India's Surveillance State: Communications Surveillance in India' [2014] SFLC <http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.> accessed 22 September 2020

[19] Ministry of Home Affairs, Government of India, 2020 <https://www.mha.gov.in/departments-of-mha> accessed 06 October 2020

matters pertaining to Home and State pertain in the said candidates, the judicial application of mind while considering requests for interception or surveillance remains missing. The decisions regarding fit cases for interception are not made by the judicial officers, but by a generalist bureaucrat with little to no experience in law enforcement and intelligence gathering. This may not only result in serious violation of rights of the citizens, when taken from the citizens' point of view, but may also result in serious ramifications for the State. For instance, if an officer entrusted with such duty being bereft legal, technical, and judicial training, scared of repercussions like being pulled for sanctioning too many requests for surveillance then chooses to reject other set of applications en masse, it can have grave implication on the security and integrity of the State.

3. Right to Privacy in the Indian Legal Framework

India's journey towards finally having the 'right to privacy' as a recognized fundamental right has rather been a long one. Starting from the roots of the Kharak Singh case,[20] which was decided in 1962, to the 2017 Justice K. Puttaswamy judgment,[21] the right to privacy has finally been declared as an inclusive part of Article 21 of the Indian Constitution.[22] The right to privacy in its full context was considered by the bench for the very first time, in the Kharak Singh case, although it was not recognized to be a right guaranteed by the Constitution.[23] The bench had connected the effect of law enforcement agencies' surveillance mechanisms on the petitioner's right to privacy. However, the bench in the PUCL case[24] pronounced the judgment in support of Justice Subba Rao's dissenting opinion in the Kharak Singh case, which lead to the expansion of the scope of Article 21, to include "right of an individual to be free from restrictions or encroachments on his person".[25]

The Kharak Singh judgment further went on to relate physical restraint with physical encroachment, stating, if the former affects one's personal liberty, the latter is equally set to affect their private life. It clarified that nothing remains more important to an individual holding a calculated interference with their privacy. And in this context, the bench had declared,

> *"we would, therefore, define the right of personal liberty in Art. 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures*".[26]

The Kharak Singh case closely followed the examination of the American Fifth and Fourteenth Amendments, which guarantees life, liberty and property, and is followed by the examination of the Fourth Amendment, which protects a person from unreasonable

[20] *Kharak Singh v. State of Uttar Pradesh* [1964] 1 SCR 332
[21] *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Others* [2017] 10 SCC 1 503
[22] Constitution of India 1950, a 21
[23] *Kharak Singh v. State of Uttar Pradesh* [1964] 1 SCR 332, [15]
[24] *People's Union for Civil Liberties v. Union of India* [1997] 1 SCC 301, [18]
[25] *Kharak Singh v. State of Uttar Pradesh [1964] 1 SCR 332, [28]*
[26] Ibid 28.

searches and seizures. The Fourth Amendment ambiguously admits that the Constitution contains no like guarantee,[27] but holds nonetheless that

> "*an unauthorised intrusion into a person's home or the disturbance caused to him thereby, is as it were the violation of a common law right of a man - an ultimate essential of ordered liberty*".[28]

This jurisprudence, however, has been based on the common law of trespass, where a person's property was held sacrosanct, and not open to be trespassed against. Almost four years after the Kharak Singh case was decided, in Katz,[29] the US Supreme Court shifted its own jurisprudence to hold that the Fourth Amendment protected zones where persons had a "*reasonable expectation of privacy*", as opposed to simply protecting listed items. Kharak Singh case was handed down before Katz, yet it expressly showed that the rulings in Katz were well anticipated in expressly grounding article 21's personal liberty right within the meaning of dignity.

In the coming decades, the PUCL case then highlighted the issue of the right to privacy in the context of elevating it to a Constitutional status. The bench, therefore, relied on the decision in R. Rajagopal v. State of Tamil Nadu ('Rajagopal'),[30] which held that the right to privacy was an implicit aspect under the right to life and liberty, as was guaranteed to all the citizens of the country, under Article 21.[31] The Court in Rajagopal's case also went a step forward to expand the concept of the right to privacy, and included the "right to be let alone" and "safeguarding the privacy of another".[32]

The PUCL case, hence, succeeded in showing the evolution of the Supreme Court's conception of privacy. In this way, the 'right to privacy' was expanded beyond the physical realm to include personal communications. It was held that an individual's right to have a telephonic conversation in the privacy of their home or office without any interference could be claimed as their right to privacy.[33] However, in the contemporary context, it can rightfully be understood that this evolving paradigm of privacy equally encompasses online communications under its bracket.

3.1. Indian Judiciary and Surveillance

Indian Judiciary in its various judgements has dealt with surveillance issues, which have been highly prominent in determining the privacy landscape in India. The Indian Supreme Court in *Hukam Chand Shyam Lal* v. *Union of India* interpreted the scope of section 5 of the Telegraph Act and held that the existence of "emergency", which is a prerequisite for the exercise of power to take possession of any telegraphs must be a "public emergency" and not any other kind of emergency. The court further clarified that the scope of "public emergency" relates to the situations contemplated under the sub-section pertaining to "*sovereignty and integrity of India, the security of the State, friendly relations with*

[27] *Wolf v. Colorado* [1949] 338 US 25, [2]
[28] *Kharak Singh v. State of Uttar Pradesh* [1964] 1 SCR 332, [15]
[29] *Katz v. United States* [1967] 389 US 347
[30] *R. Rajagopal v. State of Tamil Nadu* [1994] 6 SCC 632
[31] *R. Rajagopal v. State of Tamil Nadu* [1994] 6 SCC 632, [28]
[32] *R. Rajagopal v. State of Tamil Nadu* [1994] 6 SCC 632, [26]
[33] *People's Union for Civil Liberties v. Union of India* [1997] 1 SCC 301, [18]

foreign States or public order or for preventing incitement to the commission of an offence".[34]

Alongside the same, one other major issue with the prevailing laws on surveillance is its concentration of power exclusively within the executive branch of the government. The Court in *PUCL* v. *Union of India* did not impose the prior requirement of a case-by-case judicial standing for requests of surveillance, and left this important gatekeeping to the executive branch.[35] However, the need to revisit this considering it contravenes the very principle of separation of powers, creating a conflict of interests within the executive, as the executive itself is responsible for both, surveillance of an individual and deciding whether intercepting of that individual's telecommunication would be just in law and reasonable of his fundamental rights. Therefore, with the most basic rights of lakhs of citizens being at stake, which was not arguably the case when the PUCL was decided, it remains important that every application of request of surveillance be evaluated individually with a broader application of judicial mind, to determine whether the said application is legitimate towards justifying an infringement of one's rights or not.

The constitutional validity of Section 69A of the Information Technology Act, 2000 read with the Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, which allows blocking of access to information was upheld by the Supreme Court in the case of *Shreya Singhal* v. *Union of India*.[36]

In *Anuradha Bhasin v. Union of India,*[37] the Hon'ble Supreme Court has reiterated and explained the scope of ban/restriction on Internet imposed by the State and its rationality and constitutionality. The court also laid emphasis and recognized the fact that modern terrorism heavily relies on internet and realized the need to be vigilant and careful in handling such a powerful and effective tool.[38]

The Hon'ble Supreme Court has implicitly upheld selective government action and interception through internet to stop terrorism using the means of internet and its regulation and surveillance rather than to impose a blanket ban on internet over any area or to adopt stringent law for counter-terrorism measures. Even though the Indian Judiciary has felt the importance of imposing reasonable restrictions on the right to privacy and the importance of the evidentiary values of such information obtained through Interception and Surveillance, it has still shown reluctance in realizing the raising need for stringent Surveillance laws in the country to curb the incessant increase in threats to National Security.[39]

[34] *Hukam Chand Shyam Lal v. Union of India* [1976] 2 SCC 128, [13]-[16]
[35] *People's Union for Civil Liberties v. Union of India* [1997] 1 SCC 301, [35]
[36] *Shreya Singhal v. Union of India* (2015) 5 SCC 1, [116], [119]
[37] *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637 [150]
[38] *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637 [43]
[39] *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637 [45]

4. Surveillance Laws in the US and the role of US Judiciary:

"Terrorism is escalating to the point that citizens of the United States may soon have to choose between civil liberties and more intrusive forms of protection".[40]

Ratified in 1791, the Fourth Amendment of the US Constitution provided the basic framework for the protection of citizen's personal communication from intrusion by the government. Right to Privacy was first recognised as a part within the Fourth Amendment in 1886 by the US Supreme court in the case of *Boyd v. United States,*[41] where the court held that it is inappropriate to trespass a person's liberty through inspection of his personal communications.

At first, the US Judiciary did not recognise the need to ensure a proper separation of powers and its role in protecting in the rights of individuals from "unreasonable searches and seizures" from the government as provided by the Fourth Amendment.[42] However, with the raising growth of the field of electronic surveillance, the United States Judiciary realised its role to balance substantial constitutional concerns between the right to personal liberties and privacy of its citizens with the security concerns and interests of the US government.

The US Judiciary initially held that electronic surveillance/eavesdropping was not a search or seizure implicated in the Fourth Amendment in the case of *Olmstead v. U.S (1928)*[43] as the government intercepted information without entering the place of surveillance. The Supreme Court held that due to the essential elements of entry, search and seizure involved in the interception of the communication, the Fourth Amendment did not protect telephonic conversations.[44]

Following the Court's decision in this case, the Congress enacted the Communications Act[45] in 1934, which states that no person (unless authorised) shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person, and that anyone possessing such intercepted communication shall not make use of the same for their own benefit or for the benefit of another not entitled thereto. However, in *Katz v. United States,*[46] the Supreme Court overruled *Olmstead* and held that electronic surveillance is constitutional but only when such measures are bound by procedural safeguards which justifies the same and held that the Fourth Amendment protects any place maintainable as an exception of privacy which is reasonable. The Court held that "the Government's activities in electronically listening to and recording the petitioners' words violated the

[40] Col. Thomas W. McShane, 'Life, Liberty and the Pursuit of Security: Balancing American Values in Difficult Times' [2001] PA. LAW 46
[41] *Boyd v. United States* [1886] U.S. 616, [116]
[42] Jie Xiu, 'The Roles of the Judiciary in Examining and Supervising the Changing Laws of Electronic Surveillance' [2003] 28 Seton Hall Legis J, 229
[43] *Olmstead v. United States* [1928] 277 U.S. 438, [465]-[466]
[44] *Olmstead v. United States* [1928] 277 U.S. 438, [466]
[45] Pub. L. No. 73-416, 48 Star. 1064 [1934]; 47 U.S.C. § 605 [2000].
[46] *Katz v. United States* [1967] 389 U.S. 347, [359]

privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment".[47]

As a legislative response to this case, Title III was enacted by the Congress.[48] Pursuant to this legislation, before engaging in activities of surveillance, law enforcement agencies are required to obtain warrants for investigation[49] and for such a warrant to be granted by the judge, he must be convinced that an apparent cause exists and that a grave crime has been or is about to be committed,[50] thus laying a substantial ground of protection against unreasonable searches and seizures. Title III provided a broader scope of not interfering the surveillance activities of the executive over matters of foreign intelligence.[51]

Initiating the establishment of Surveillance Laws in the US, in 1968, Congress passed a federal wiretapping statute in Title III of the Omnibus Crime Control and Safe Streets Act in response to the Supreme Court's criticism of the statute in Berger v. New York,[52] where the court struck down the New York statute which authorized the law enforcement agencies to eavesdrop electronic communications and mounting public awareness of the government's illegitimate use of wiretaps.[53] By passing Title III, the Congress authorized law enforcement officers with the ability to efficiently be vigilant towards anti-governmental activities, while balancing the corresponding privacy of innocent people.[54] In order to keep itself in level with the perpetual advances and improvements made to communication technologies, the Congress continually kept amending Title III.[55]

It was not until 1972, in the case of *United States v. United States District Court,*[56] the US Supreme Court first addressed the problems related to national security and surveillance and allowed the Congress to formulate standards and guidelines for domestic security wiretaps, however holding that the President should exercise his executive authority within the limitations under the Fourth Amendment.[57] The Court, while examining the Fourth Amendment considering the executive authority of warrantless foreign intelligence surveillance, recognised an inherent national security exception in exercising such authority and held it to be constitutional.[58]

The Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA), which widened the executive branch's Title III powers for search and seizure with regards to foreign enemies, responding to the inclined threat to national security from abroad.[59] By passing FISA, the Congress authorized the Executive Branch to conduct authentic

47 *Katz v. United States* [1967] 389 U.S. 347, [353]
48 Jie Xiu, 'The Roles of the Judiciary in Examining and Supervising the Changing Laws of Electronic Surveillance' [2003] 28 Seton Hall Legis J, 229
49 18 U.S.C. 1994, s 2518(3)(a)
50 18 U.S.C. 1994, s 2516(1)
51 18 U.S.C. 1994, s 2511(2)(e)(f)
52 *Berger v. New York* [1967] 388 U.S. 41, [44], [51], [59]-[60]
53 Pub. L. No. 90-351, Title 111, 82 Stat. 197, 211 [1968]
54 Barry D. Roseman, 'Electronic Platform, E-mail and Privacy Issues', [2001] SGO16 A.L.I.-A.B.A. 1165, 1166-67
55 Barry D. Roseman, 'Electronic Platform, E-mail and Privacy Issues', [2001] SGO16 A.L.I.-A.B.A. 1165, 1167-68
56 *United States v. United States District Court* [1972] 407 U.S. 297, [299]
57 *United States v. United States District Court* [1972] 407 U.S. 297, [321]-[323]
58 *United States v. Truong Dinh Hung* [1980] 629 4th Cir. 908, [912]-[913]
59 Pub. L. No. 95-604, at 3904, 3916 [1977].

electronic surveillance for foreign intelligence[60] tenacities within the context of the nation's obligation to privacy and individual rights. When such inherent powers given for foreign intelligence activities were challenged based on its constitutional validity in the case of *United States v. United States District Court*,[61] the Supreme Court emphasized on the necessity of judicial interventions in concerned matters of Surveillance conducted for National Security pursuant to FISA and provided more effective checks and balances on the executive authorities. However, the court also provided a discrete justification for surveillance activities nevertheless leaving many issues unanswered.[62]

Title III was further amended by the Congress by passing the Electronic Communications Privacy Act of 1986 (ECPA) which served as a domestic surveillance legislation in response to the increasing technological developments and use of computers, internet and cellular telephones for emails and other communication purposes. The ECPA institutes a judicial controlled procedure to permit surveillance and interceptions for law enforcement purposes.[63] The Act made Title III applicable to trap-and-trace devices, voice mail and e-mail messages, and other forms of electronic and digital communications, such as radio transmissions, telegraphs, wire communications, etc. In its Second Report and Order of 2006, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) mandated the telecommunications companies to cooperate and support all the efforts taken with the targeted electronic surveillance initiatives of the Government and such cooperation may include modifications to the design of equipment, facilities, and services.[64]

On October 26, 2001, United States President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (hereinafter PATRIOT Act)[65] within 6 weeks of the 9/11 terror attacks, which provided autonomy to investigating agencies to employ surveillance measurers to counter anti-national and terrorist activities, while instantaneously dropping judicial regulation and accountability for the same. By expanding the ability and authority of the government for carrying out electronic surveillance, the PATRIOT Act ensured the government's authority to monitor and sabotage indefinable terrorist network groups domestically and across international borders.[66] The PATRIOT Act removed the enforcement barriers for the intelligent agencies by granting additional wiretapping and surveillance authority. For example, section 106 of the PATRIOT Act allows the President to summarily confiscate and sell the assets and property of foreign nationals he determines were responsible for attacks on the United States; section 210 of the Act allows investigators to intercept telephone and ISP records and section 214 allows governmental trap and trace orders.

60 50 U.S.C. 1994, s 1804(a)(4)(A)
61 *United States v. United States District Court* [1972] 407 U.S. 297, [299]
62 Michael F Dowley, 'Government Surveillance Powers under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time - A Constitutional Tug-of-War' [2002] 36 Suffolk U L Rev 165
63 18 U.S.C. 2510-2522
64 'Electronic Surveillance', Legal Information Institute, Cornell Law School <https://www.law.cornell.edu/wex/electronic_surveillance#footnote2_nhopdas> accessed 30 August 2020
65 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 [2001].
66 Lt. Col. Joginder S. Dillon & Lt. Col. Robert Smith, 'Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques', [2001] 50 A.F. L. REV. 135, 148

Even in its most recent instance, the US Supreme Court in *Timothy Ivory Carpenter v. United States*[67] measured the state's exercise of police powers against a citizen's right to privacy and held that government access of mobile phone records was indeed a Fourth Amendment search, which include the safeguard of certain expectations of a person's privacy. This proves that the US Judiciary felt the need and importance of inculcating stringent measures of Surveillance for protecting the interests of the state and for national security and to balance the same with the individual's right to privacy.[68] Thus, the US government possesses significant amount of authority over matters of national security, public welfare, state's interest, and defence although there exists certain radius of constitutional limitations.[69]

5. The need for the enactment of stringent laws in India

In comparison to the laws in India, the model followed in the United States requires a prior judicial intervention for the authorization of wiretapping, interception or other ways of surveillance. The procedure for the same is followed in similar lines to that of a judge issuing warrants of search or arrests.[70] Although the scheme as followed in the United States can seem to be the most content to protect the rights of the citizens and attractive on the human rights' front, however, it could be debatable to have this followed in the Indian context considering the overburdened segment of the judiciary with higher rates of pendency than ever along with the vacancies.[71]

The purpose for recognizing the US legal system as a frame of reference to equate and analyze the Indian position is primarily because much like India, America has also been facing a tremendous revolutionary change in its legal system with respect to privacy issues and surveillance post the 9/11 attacks, which laid the foundation of the PATRIOT Act. Similarly, post 26/11 Mumbai terror attacks, India observed unprecedented changes in its anti-terrorism measures to provide greater autonomy to the investigating agencies.

5.1. The Menace of Terrorism and absence of effective Surveillance laws

> *"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner".*[72]

[67] *Timothy Ivory Carpenter v. United States* [2018] 585 U.S.
[68] Nehaa Chaudhari, Smitha Krishna Prasad, 'Carpenter v. United States: State Surveillance and Citizen Privacy' [2019] 13 NALSAR Stud L Rev 129, 133-135, 143-146
[69] Col. Thomas W. McShane, 'Life, Liberty and the Pursuit of Security: Balancing American Values in Difficult Times', [2001] PA. LAW 46
[70] Solove, Daniel J, 'The First Amendment as Criminal Procedure' [2007] 82 NYU L Rev 112, 154–59
[71] Gowda, Sadananda, 'Pending Court Cases: Written Reply by Union Minister of Law and Justice, Government of India in the Lok Sabha, 3 December, 2015, 16th Lok Sabha' [2015] Lok Sabha Debates, Parliament of India
[72] Ban Ki-moon, <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 04 March 2021

> *"Terrorist organizations have also begun to employ websites as a form of information warfare which disperses inaccurate material which triggers scandalous consequences".*[73]

Contemporary terrorism heavily depends on internet. Operations on the internet are not easily traceable and this funds fallacious proxy wars and an easy inroad to young and impressionable minds. Social media platforms serve as an efficient weapon to reach young minds, to spread anti-national ideologies and recruit members. For example, the Al-Qaeda's websites carry manuals on how to construct explosive devices.[74]

India is devoid of a concrete Surveillance Law to curb this imminent issue. India requires a solid foundational law on Surveillance, which also protects the personal data and information. In fact, the gaps, and loopholes in the National Security ecosystem in India aided as an advantage for the terrorists who attacked Mumbai on 26/11.[75] There is a rising need for a wholesome law in the country, which covers the broader facets of national security and counter-terrorism measures. The laws must meet all the technical requirements based on the available capability and endure for a proper use of all the surveilled material.

The aftermath of Justice K.S. Puttaswamy judgement saw the uprooting of the Personal Data Protection Bill in 2019 which aims at balancing National Security and Privacy and restricted the authority to permit surveillance only to the Home Secretary, Ministry of Home Affairs and to the Government of India.

Richard A Posner, Senior lecturer in law at the University of Chicago, rightly observes:

> *Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defense of national security.*[76]

Comparing the U.S. Supreme Court's decision in *Thomas Ivory Carpenter v. United States* and the Indian Supreme Court's decision in *Puttaswamy v. Union of India,* it is evident to note that the Indian Judiciary has not yet identified a broad exception to the right of privacy corresponding to that of the U.S. Judiciary.[77]

The United States enacted the USA PATRIOT Act sensing the importance of a National Surveillance regime witnessing the aftermath of the 9/11 attacks in 2001. The revelations

---

[73] Gregory S. McNeal, 'Cyber Embargo: Countering the Internet Jihad', [2007] 39 Case W Res J Int'l L 789
[74] Jason Burke, 'Al-Qaeda launches online terrorist manual, [2004] The Guardian <https://www.theguardian.com/technology/2004/jan/18/alqaida.internationalnews> accessed 30 December 2020
[75] Dhaval D. Desai, Parjanya Bhatt, 'Securing India's Cities: Remembering 26/11, Learning its Lessons', [2019] ORF Special Report No. 92
[76] Richard A. Posner, 'Privacy, Surveillance, and Law', [2008] 75 Uni. of Chicago L Rev. 251
[77] Nehaa Chaudhari, Smitha Krishna Prasad, 'Carpenter v. United States: State Surveillance and Citizen Privacy' [2019] 13 NALSAR Stud L Rev 129

made by Edward Snowden, the whistle-blower, in 2013 tells us about the usage of phone companies by the US Government to collect relevant information on millions of citizens.[78] The disclosures made by Snowden were responsible for exposing the US government's scope of surveillance activities of which it became evident that India was their prominent target.[79]

On December 13, 2001, five terrorists attacked the Indian National Parliament, which resulted in killing of seven persons and placing the country into a heightened state of alert.[80] The Government of India, in March 2002, like its American counterpart, passed the Prevention of Terrorism Act (POTA), to augment India's ability to crack down on conceivable terrorist threats.[81] The Government reiterated that its action was a response to *"an upsurge of terrorist activities, intensification of cross border terrorism, and insurgent groups in different parts of the country".*[82] Section 45 of Act provided for the admissibility of evidences collected through the interception of communication. All evidence collected through the interception of wire, electronic or oral communication were made admissible as evidence against the accused in court during the trial of the case. The act also laid down various safeguards to prevent the misuse of powers by authorities against innocent persons. However, on the 17 September 2004, the act was repealed by the successive government, which came to power after the national elections.

Similarly, considering the 2008 Mumbai terror attacks, India adopted a wide range of schemes and data sharing methodologies for surveillance to enhance public safety and security and to tackle the growing crime and terrorism in the country. The Government of India amended the Information Technology Act, 2000 to provide for the offence of cyber terrorism under section 66F.

A July 2020 United Nations' Report on Terrorism revealed that there are "significant numbers" of Islamic State (IS) terrorists in India.[83] This indicates the need for strong surveillance laws. The contention of the authors is that while the U.S. Patriot Act placed new regulations on the use of governmental surveillance and sought to curtail and avoid future terrorist acts by intensifying the federal government's powers, India is yet to design a strategic framework in shape of a vigilant law to curb such activities against the state.

It is therefore clear that whichever model of governing such concerns is ultimately chosen, either an independent authority or a privacy commissioner as suggested by

[78] Sriram, Jayant, 'What are the surveillance laws in India?' [2019] The Hindu, <https://www.thehindu.com/news/national/what-are-the-surveillance-laws-in-india/article29993602.ece> accessed 01 December 2020

[79] Glenn Greenwald, Shobhan Saxna, 'India among Top Targets of Spying by NSA' [2013] <http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece> accessed 10 December 2020

[80] Rediff News Serv., 'The Attack on Parliament (2001)' <http://www.rediff.com/news/pat2001.htm> accessed 01 December 2020

[81] Prevention of Terrorism Act 2002

[82] Christopher Gagné, 'POTA: Lessons Learned from India's Anti-Terror Act' [2005] 25 B.C. Third World L.J. 261

[83] PTI, 'U.N. report flags Islamic State threat in Karnataka, Kerala' [2020] The Hindu <https://www.thehindu.com/news/national/kerala/un-report-flags-islamic-state-threat-in-karnataka-kerala/article32189443.ece#> accessed 09 December 2020

Justice A P Shah (Retd.) Committee in 2012,[84] the body shall thread its staff from the law enforcement agencies, civil society, intelligence community and the judiciary. However, while the best model is yet to be examined and designated, it would be wise to have the respective Home Secretaries be provided with a dedicated team of joint secretaries, with prior experience in security, investigations, and intelligence.

6. Conclusion

While the prospect of fashioning a model surveillance framework, which protects the privacy of individuals without compromising national security, continues to be debated, currently this seems to be the only remaining reconciliation possible between the two seemingly conflicting yet necessary ideals.[85] The government of India carries out surveillance by various authorities through its numerous laws and license agreements for service providers under its legal framework. Though the legalised, defensible, and targeted surveillance can be an effective tool in ministering law enforcement agencies in attempting to tackle crime and terrorism, an umbrella surveillance law which encompasses all requisite anti-terrorism mechanisms while adequately safeguarding individual's right to privacy and data protection is the need of the hour in India. Though the Government of India has been deploying various strategies and projects for mass surveillance activities, details of such operations and their legal safeguards are uncertain due to lack of proper verified information and lack of specific statutory backing.[86]

There is a need for a robust and comprehensive law which synchronises synergy between the states and citizens, providing undivided attention to significant problems of composing effective governmental measures and enforcement of the same. While the US has taken cognizance of the impact of technological developments which pose a major threat to national security by framing "*near perfect surveillance laws",*[87] India, on the other hand, has very limited safeguards protecting the privacy of its citizens and relatively less effective surveillance laws to protect its national security.

References

I. Cases

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

Berger v. New York, [1967] 388 U.S. 41

Boyd v. United States, [1886]] U.S. 616

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

[84] Justice A P Shah (Retd.) Committee, 'Report of the Group of Experts on Privacy' [2012] *Planning Commission*, Government of India. Available online at: <https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503> <http://www.planningcommission.nic.in/reports/genrep/rep_privacy.pdf> accessed 03 March 2021

[85] Agnidipto Tarafder, 'Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India' [2015] 57(4) ILI J. 550, 578

[86] Chaitanya Ramachandran, 'PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age' [2014] 7 NUJS L Rev 105

[87] *Timothy Ivory Carpenter v. United States* [2018] 585 U.S., [13]

Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Others, [2017] 10 SCC 1

Katz v. United States, [1967] 389 US 347

Kharak Singh v. State of Uttar Pradesh, [1964] 1 SCR 332

Olmstead v. United States, [1928] 277 U.S. 438

People's Union for Civil Liberties v. Union of India, [1997] 1 SCC 301

R. Rajagopal v. State of Tamil Nadu, [1994] 6 SCC 632

Shreya Singhal v. Union of India, [2015] 5 SCC 1

Timothy Ivory Carpenter v. United States, [2018] 585 U.S.

United States v. United States District Court, [1972] 407 U.S. 297

Wolf v. Colorado, [1949] 338 US 25

II. Articles

Arun C., 'Paper-thin Safeguards and Mass Surveillance in India' [2014] 26 NLSIR 105

Chaudhari N., Smitha Krishna Prasad, 'Carpenter v. United States: State Surveillance and Citizen Privacy' [2019] 13 NALSAR Stud L Rev 129

Desai D., Parjanya Bhatt, 'Securing India's Cities: Remembering 26/11, Learning its Lessons', [2019] ORF Special Report No. 92

Dillon J. & Smith R., 'Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques', [2001] 50 A.F. L. REV. 135

Dowley M., 'Government Surveillance Powers under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time - A Constitutional Tug-of-War' [2002] 36 Suffolk U L Rev 165

Gagné C., '*POTA: Lessons Learned from India's Anti-Terror Act'* [2005] 25 B.C. Third World L.J. 261

Kasaudhan A., 'Surveillance and right to privacy: Issues and challenges' [2017] 3 IJL 73

McNeal G., 'Cyber Embargo: Countering the Internet Jihad', [2007] 39 Case W Res J Int'l L 789

McShane T., 'Life, Liberty and the Pursuit of Security: Balancing American Values in Difficult Times' [2001] PA. LAW 46

Posner R., 'Privacy, Surveillance, and Law', [2008] 75 Uni. of Chicago L Rev. 251

Ramachandran C., 'PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age' [2014] 7 NUJS L Rev 105

Roseman B., 'Electronic Platform, E-mail and Privacy Issues', [2001] SGO16 A.L.I.-A.B.A. 1165

SAHRDC, 'Architecture of Surveillance' [2014] 49 EPW 10

Schauer F., 'Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"' [1978] 58 BU L Rev 693

Solove, Daniel J, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 44 SD L Rev 771

Solove, Daniel J, 'The First Amendment as Criminal Procedure' [2007] 82 NYU L Rev 112

Tarafder A., 'Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India' [2015] 57(4) ILI J. 550

Xiu J., 'The Roles of the Judiciary in Examining and Supervising the Changing Laws of Electronic Surveillance' [2003] 28 Seton Hall Legis J

III. Online Sources

'Electronic Surveillance', Legal Information Institute, Cornell Law School <https://www.law.cornell.edu/wex/electronic_surveillance#footnote2_nhopdas> accessed 30 August 2020

Ban Ki-moon, <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 04 March 2021

Burke J., 'Al-Qaeda launches online terrorist manual, [2004] The Guardian <https://www.theguardian.com/technology/2004/jan/18/alqaida.internationalnews> accessed 30 December 2020

Dash Z., 'Do Our Wiretapping Laws Adequately Protect the Right to Privacy?' [2018] 53(6) E&PW <https://www.epw.in/engage/article/can-government-continue-unhindered-wiretapping-without-flouting-right-privacy> accessed 06 October 2020> accessed 16 February 2021

Greenwald G. & Saxena S., 'India among Top Targets of Spying by NSA' [2013] <http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece> accessed 10 December 2020

J. Shah A. (Retd.) Committee, 'Report of the Group of Experts on Privacy' [2012] *Planning Commission*, Government of India, <https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503> and <http://www.planningcommission.nic.in/reports/genrep/rep_privacy.pdf> accessed 03 March 2021

Ministry of Home Affairs, Government of India, 2020 <https://www.mha.gov.in/departments-of-mha> accessed 06 October 2020

PTI, 'U.N. report flags Islamic State threat in Karnataka, Kerala' [2020] The Hindu <https://www.thehindu.com/news/national/kerala/un-report-flags-islamic-state-threat-in-karnataka-kerala/article32189443.ece#> accessed 09 December 2020

Rediff News Serv., 'The Attack on Parliament (2001)' <http://www.rediff.com/news/pat2001.html> accessed 01 December 2020

Rizvi K., 'Personal Data Protection Bill 2019 and Surveillance: Balancing Security and Privacy', [2020] INC42 <https://inc42.com/resources/personal-data-protection-bill-2019-and-surveillance-balancing-security-and-privacy/> accessed 06 March 2021

SFLC, 'India's Surveillance State: Communications Surveillance in India' [2014] *SFLC* <http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.> accessed 22 September 2020

Sriram J., 'What are the surveillance laws in India?' [2019] The Hindu, <https://www.thehindu.com/news/national/what-are-the-surveillance-laws-in-india/article29993602.ece> accessed 01 December 2020

Stakeholder Report, 'The Right to Privacy in India' [2016] UPR CIS India and Privacy International, <https://www.upr-info.org/sites/default/files/document/india/session_27_-_may_2017/js35_upr27_ind_e_main.pdf> accessed 08 March 2021

Xynou M., 'Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles' [2015] CIS <https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf> accessed 06 March 2021

IV. Legislations and Statutes

Constitution of India, 1950

Indian Telegraph Act, 1885

Personal Data Protection Bill, 2019

Prevention of Terrorism Act, 2002

The Information Technology (Amendment) Act, 2008

The Unlawful Activities (Prevention) Act, 1967

United States Code, 1994