Invasion Of Privacy Through Search and Seizure of Electronic Media: Comparative Study of USA and India

Shruti Singh[1], Kshitij Bharat Gimhavanekar[2], Dr. Aparajita Mohanty[3], Abhinav Shrivastava[4*], Raj Varma[5]

[1] LLM Scholar, Symbiosis Law School Pune (SLS),
[2]LLM Scholar, Symbiosis Law School Pune (SLS),
[3]Associate Professor, Symbiosis Law School Pune (SLS),
[4]Assistant Professor, Symbiosis Law School Pune (SLS),*
[5]Assistant Professor, Symbiosis Law School Pune (SLS), Symbiosis International (Deemed University) (SIU), Viman Nagar, Pune, Maharashtra, India

[4]Email Id: abhinav.shrivastava@symlaw.ac.in*

Abstract

With the recent development in the legal status of privacy, included as a part of fundamental right and with the coming up of various Data Protection Bills since 2019, the protection of data and privacy issues has gained major limelight. It is pertinent to acknowledge that when the lives of the people are shifted to digital medium for everyday functioning, there is an urgent necessity to have a robust legislation which can protect privacy rights of the individuals. In current times, Electronic surveillance conducted by the government is getting attention as such measures have neither legislative backing nor due process. This Research paper revolves around the development of privacy laws in India and U.S and studies how with the growth in information technology, the nature of crime has taken a digital recourse and as a counter-act, the governmental agency's use of technology turns out to be an excessive coercive action infringing the privacy of the citizens. It discusses the idea of balancing the privacy rights with the state's interest and as a result creating a safe environment for the citizens.

Keywords- Data, Privacy, Fundamental Rights, Information Technology, Surveillance.

Introduction

The right to conduct search and seizure is an indispensable part of the investigation and criminal justice system. The role played by the state in securing and maintaining peace and harmony in society indirectly provides the state the authority to perform all required functions. With globalization, technology has grown out of existing legal frameworks and has become a part of human's daily life; the digitally stored information includes every intrinsic part of life which as a result can be a major site for governmental agencies to investigate. Data Surveillance is a worldwide phenomenon conducted by private and government entities. Technology strengthens the State to peek into the lives of the citizens and creates a large-scale privacy issue and authorization to various States to keep a check on the citizens is making the state a "surveillance state"

Right to privacy was not considered as a fundamental right in India until 2017 after Puttaswamy's judgment wherein the right to privacy was accepted by the Supreme Court and it was included as an intrinsic part of the fundamental right which is right to life and personal liberty under Article 21 of the Indian Constitution. There is a need to restore the balance and uphold individual rights, in this regard; the model projected by the United States can be very helpful and be an inspiration that we might look up for as it provides the protection of the fourth amendment. With the advancement in privacy rights, we have moved in the direction of United States i.e., a correct step by providing protection to privacy rights and consequently we should likewise assess the connected improvements in the U.S and other comparative arrangements to guarantee a positive and smooth change. The Fourth Amendment to the U.S Constitution, 1792 states that "People have a right to be secure in their persons, houses, papers, and effects against unreasonable searches and seizure". It restricts the government's unlimited right to perform searches and seizures and guarantees that citizens have a "reasonable expectation of privacy."

It becomes crucial to understand the expansion of information technology in methods of search and seizure conducted by governmental agencies in India and U.S. and to study how the surveillance by the State is infringing the right to privacy of the citizens along with the measures to handle it. This research is based on literature already available hence the researchers have further analyzed the information. An attempt has been made to understand

whether with the advancement of technology, the outdated provisions related to Search and Seizure of electronic devices will be able to uphold the privacy rights of individuals or the surveillance laws in India need to be re-designed. The paper discusses the evolution of privacy laws from physical search to internet surveillance with different parameters set for privacy in India and USA and proposes a system where accountability and responsibility of the government is to be increased with reasonable checks and balances creating a proper process of judicial scrutiny in the procedure of search and seizure.

The privacy laws have evolved in India [1] through judicial interpretation in the Kharak Singh case where it was held that personal liberty is grounded within the meaning of dignity, attaching it to the persons and not the places to Justice Puttaswamy case wherein right to privacy has been recognized as a fundamental right. The Aadhar judgment was further discussed [2] where it is concluded that the court gave a narrow interpretation regarding an individual's privacy rights wherein it only evaluated the immediate problems caused due to infringement and neglected the opportunity to address the long-term data privacy issue and imbalances in society. The design is in favour of privacy with fewer exceptions, but in reality, the exceptions are used for the abuse of power by the government agencies and private institutions. The judgment also ignored how State Resident Data Hubs (SRDHs) can be an easy tool for big data analytics and profiling. Ramachandran [3] analyses a thorough re-examination of privacy laws in India. The judgment of PUCL v UOI is scrutinized and it is concluded that there is a major shift in the dependence on the internet resources now people's whole life is on the internet. The present guidelines regulating mass surveillance is vastly influenced by guidelines set in PUCL. It is a fact that outdated privacy laws can not keep up with the new digital age and surveillance projects which are deployed by the government. The General Data Protection Regulation (GDPR) which is a regulation in European Union on data protection and privacy along with other regulatory areas, such as DNA technology, finance, and telecom and other laws such as Information Technology Act, 2000 and Aadhaar Act, 2016 was further discussed [4]**.** In the United States, the Fourth Amendment provides protection to the citizens from any unwarranted search and seizure [5] discusses the increase in digital surveillance conducted by the government and throws light on a possible solution where a two-tier system can be adopted to create a stability between an individual's privacy rights and the practical needs of governmental agencies. If any digital surveillance is adequately invasive of an individual's privacy, the government must obtain a warrant backed by probable cause whereas fewer invasions would require only reasonable suspicion. Finally, another promising point of research would be that it studies the increase in the frequency of constitutionally problematic acts and whether the number of individuals affected by it makes any difference, it was concluded that the increase in the occurrence of invasive surveillance may result in greater intrusion of privacy of all. Slobogin [6] **and** Sculhofer [7] describes how with the help of new technologies, the government can easily monitor the citizens from data mining to airport scans to drug testing; privacy is under attack like never before. It is argued that there is a need for a stronger legislative framework to stop this executive overreach by placing a balanced regulatory regime. Further elaborating on the subject matter Smith [8] presents that there has been grave violation of an individual's privacy as the United States Department of Homeland Security (DHS) conducts surveillance on digital contents of electronic devices of citizens and non-citizens crossing international borders. Post 9/11 the attack, there has been a serious threat to national security resulting in liberty restrictions. Research has provided evidence that the border exception of the fourth amendment is used to rationalize warrantless scrutiny of personal digital documents which has resulted in swallowing the rule itself. "The digital life of an individual ought not to be hijacked just by crossing a border". This has been previously assessed only to a very limited extent because laptops and other digital devices are considered as luggage but therefore there is a low expectancy of privacy. Recently in 2019, in the case Alasaad v. Nielsen, Judge Casper held that a border agent should have "reasonable suspicion" that a device accommodates digital contraband before searching or seizing the device. Line search exemption for the necessity of warrant applies just to routine searches, however searches of individual electronic devices are arranged into non-routine searches as it abuses the first and fourth amendment. The exceptions provided to such search and seizure gives a lot of scope for privacy invasions, Gliksberg [9] explains how the government uses the third-party exemption if a warrant is necessary to get to the data with the reasoning that the disclosure to a third-party (Service provider) absolves privacy issues. There exists a considerable body of literature that relies on the principle of 'reasonable expectation of privacy which the society can recognize'. Gregory [10] in his book elaborated about how modernization in the technological field brings out both an opportunity and threat. The Fourth Amendment to the US Constitution clearly requires a warrant for all searches and seizures and that the government policy at odds with this doctrine violates the Constitution. Moreover, the question that is dealt with is whether the amendment requires a warrant for all seizure and search or whether there is prohibition of unreasonable search and seizure. However, without a clear definition of the word 'reasonable' it is left with the Court's interpretation to extend its meaning. Considering the two preferences there arises two concepts of the amendment one that is warrant preference and another reasonable interpretation. In the 21st century, the Courts have given dominance to the warrants for searches as regards reasonable interpretation.

In matters where national security is involved, the executives should not be neutral as that of a Court or Magistrate. The Constitution requires a strict check and balance on warrantless wiretapping even in the name of national security. It was also argued that the courts should either adopt third-party doctrine or abolish the same altogether. While analyzing the Fourth amendment of the US constitution, it was discussed that if the fourth amendment rights are solely based on the concept of property, then they lose the strongest argument against wiretapping.

It has been observed in the above-mentioned literature that there is an increase of understanding of privacy in India. The research on the surveillance conducted by the government is still at a very nascent stage in India as privacy after years of debates is now formally recognized as an intrinsic part of Right to life and personal liberty. The gap in the existing literature is that there is no relevance put on the need for statutory backing to the surveillance projects and case to case review by the judiciary to create the balance between the executive and judiciary. The legal system needs a sounder judicial model to access technological advancement and to have a holistic approach to protect privacy rights. The physical seizure and digital search of privacy should be respected in different manner because they connote completely different levels of privacy issues therefore, following the same parameters will only bring out arbitrariness as they are too far apart to be put on the same side of the coin. Also, applying the outdated legislation to the recent technologies is vague; there is a need to recognize the transformation which the new digital technologies are bringing and accordingly give protection to encryption security under the fourth amendment as citizens have a reasonable expectation of privacy.

Evolution Of Privacy Laws in India and the USA

In India, there is no legislation or any regulation which directly deals with the right to privacy of individuals. Right to privacy is an aspect of fundamental rights like right to life and personal liberty which is enshrined under Article 21 of Indian constitution. Every individual deserves to live a noble life and it could be maintained only if right to privacy will be treated as a primary necessity of a right to life and personal liberty which is why right to privacy is a significant factor for the enjoyment of life.

There are various precedents by the Supreme Court in which there is specialized development of right to privacy in India. In *K. S. Puttaswamy vs Union of India* nine judge-bench of the Supreme Court delivered the anonymous judgment regarding right to privacy. It is very important to discern that previously, the right to privacy was considered as a “common law right” before it was discussed in the Puttaswamy case. It was stated by the Supreme Court that “Life and personal liberty are not creations of the Constitution. These rights are recognized by the Constitution as inheriting in each individual as an intrinsic and inseparable part of the human element which dwells within. Privacy is a constitutionally protected right which appears predominantly from the guarantee of life and personal liberty in Article 21 of the Constitution [11]. In a case *Kharak Singh vs State of Uttar Pradesh*, the appellant of this case tortured by the UP police forces under the regulation of 236 (b) of U.P regulation permits devoted visits at night Supreme Court in this case held that 236 (b) of U.P regulation violative to article 21 of Indian constitution. The Supreme Court concluded that article 21 of the constitution includes the right to privacy for the protection of personal life and personal liberty. In this case Justice Subba Rao stated that the concept of Liberty is comprehensive and vast and the right to privacy is like the base of a concept of personal liberty therefore it is important and very mandatory to include the right to privacy in article 21 of Indian constitution [12]. In the case State vs Charulata Joshi held that article 19(1) (d) confers freedom of speech and expression. Under this article freedom of press is developed and evaluated in various manners. Justice Jaspal Singh stated that it is necessary that consent should be obtained by appraising an individual before interviewing them. The willingness of a person is very important to the aspect of right to life and personal liberty [13]. In People's Union for Civil Liberty vs union of India [14] the Supreme Court held that under the Telegraph Act telephone tapping amounts to be a violation of article 21 of Indian Constitution. The Personal Data Protection Bill, 2019, is in line with the privacy law in India which is affected by overall enhancements similarly as the individual country’s ensured law. The Constitution of India doesn't explicitly refer to privacy; but bridging the gap courts have stated that an improvement to privacy laws under the light of fundamental right which is given in Article 21.

The United States has passed various laws relating to protection of privacy of an individual. With the growing age of the information technology department, it is very important to have a check on the privacy of an individual. Development and evaluation started with the 4th amendment in the United States. Various rules and regulations show the evolution and development of privacy law in the United States. Modern technology has proved to bring both opportunities and threats that can change humanity qualitatively. Having said this, the issue which is to be dealt with is the conflicting interest between individual rights and the right to limit the state's interference in private matters. The Fourth Amendment to the US Constitution says that the search is to be made of material things like the person, the house, his papers or his effects. It clearly requires a warrant for all searches and seizures and that the government policy at odds with this doctrine violates the Constitution. Hence, it prohibits all warrantless searches.

Moreover, the question that is dealt with is whether the amendment requires a warrant for all seizure and search or whether there is prohibition of unreasonable search and seizure. Considering the two preferences there arises two concepts of the amendment, one that is warrant preference and another reasonable interpretation. In the 21st century, the Courts have given dominance to the warrants for searches as regards reasonable interpretation. The main objective of the Privacy Act, 1974 is to protect information being misused by an individual. it secures the information that would be recovered by an individual through their names and other personal identification also prevents set information from being disclosed and misused without retaining consent of an individual. It was a necessary step which shows evolution and development of the right to privacy. Telephone Record and Privacy Protection Act, 2006 applies on individual upon imitation of individual in order against personal information that is pretexting it also protects buying or selling of personal phone records of an individual and specially this does not affect any law officials or information agencies.

Globalization Of Technology and Infringement of Privacy Through Search and Seizure by Electronic Media

Globalization has played a major role to intensify the advancement of technology across the borders by allowing nations to gain an easier approach to different foreign languages and by increasing the competitiveness across borders. Every person's life is concatenated with information technology via use of computers and internet as it can be witnessed through mushrooming of internet penetration even in developing countries. The usage of information technology has shifted from consumption to participation [15]. These technologies are used to send and receive emails, to collect and preserve data; in essence people's lives are on their computer system preserving most intimate details of people's lives [16].

This technological revolution is not a secret to people who are involved in crimes therefore the laptops, phones and other kinds of communicating devices are frequently used to commit a number of criminal activities. It can be used as a means to give effect to a crime or can be used to store evidence associated with it. For example, a simple smart phone can now act more than a communicating device as it can preserve communication records, pictures, videos and documents etc. The budding dependency on such devices comes with exponential growth in crimes related to it. These high-tech crimes require prosecutors and law enforcement agencies to be attentive of the new technologies and to know how to collect electronic evidence stored in computers. The information stored in these devices could be very essential for the appropriate investigation and therefore more and more importance is given to use of warrants to search and seizure. This weakness of the law implementation offices to balance with the utilization of innovation brings about utilization of inordinate coercive state capacity to keep up harmony and security by eliminating criminals, compared with the person's entitlement to make sure about their privacy.

With the COVID 19 pandemic, the world is now relying more on devices connected to the internet for everyday functioning therefore a need for robust data protection legislation is imperative. This need became more obvious with the recognition of the right to privacy being a fundamental right by the Supreme Court of India [17]. The government has several legal routes to conduct surveillance on their citizens and the law governing till 2018 was Indian Telegraph Act, 1885, which deals with interception of calls and the Information Technology Act, 2000, which deals with interception of data. As a result, the government is provided with limited powers whereas private actors are completely barred from conducting any kind of surveillance. The IT Act also prohibits hacking and Section 43 and 66 respectively covers both civil and criminal offences of data theft and hacking. Earlier, any citizen's personal data was regulated by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under Section 43A of the Information Technology Act, 2000 [18] . The rules states definition of personal data that it includes medical records, biometric information, passwords, financial data and sexual identification [19] and affirms that only the competent authority can give directions for interference, observing and decoding of any data. The Data Protection Bill was drafted in 2019 by a committee chaired by Justice Srikrishna. It supports the structure and provisions laid down by the European Union in its General Data Protection Regulation (GDPR) as well it is in consonance with the recent landmark judgement of Aadhar [20]. The 2019 bill has given significance to consent and protects autonomy of an individual's data, by constituting a regulatory body to administer information processing activities. It provides protection from privacy breach from companies but is deficient of providing protection against 'blanket surveillance' by the government. The exemptions provided to the government to breach an individual's privacy under national security is widely arbitrary. The recent instances of information robberies in the Business Processing Outsourcing (BPO) have heaved concerns about security of information of the citizens of India. Where provision of Information Technology Act, 2000, reveals to which party can access the information but it doesn't address the need for a clear and strict legislation.

The Intelligent agencies of U.S. and U.K uses extensive surveillance systems like PRISM and TEMPORA to keep an eye on its own citizens, similar episodes are happening in India, Central Monitoring System (CMS) also provides collection of telephonic data by tapping [21] and Netra system uses keywords to spot certain specific communications. These programs doubtful statutory backing and infringes basic fundamental rights of the citizens. In the U.S, Electronic surveillance is regarded as a search under the fourth amendment which protects citizens from unreasonable search and seizure therefore it is of paramount importance for the government to obtain warrant from the court of law and ascertain that there was a probable cause to believe to conduct such search with fewer exceptions for difficult situations.

After the terrorist attack of 9/11 in the year 2001, USA PATRIOT (Uniting and Strengthening America by Providing its Appropriate Tools needed to be Intercept and Obstruct Terrorism) Act was voted for which gave permission to the government to gather telephonic data which was revealed by the whistleblower Edward Snowden in 2013. In Carpenter vs. United States [22], the apex court recognized a principle where it was necessary for the government to obtain a warrant before accessing information from users generated by cellphones of a suspect in a criminal investigation. It curtails unrestricted power of the government to look into wireless databases. In United States v. Miller [23], the third-party doctrine was enunciated that if a person reveals his confidential information to a third party, the expectation of his privacy stops there even if he revealed that information on the assumption that it will be used for a limited time period, the government can obtain the information directly through the third- party but Collector v. Canara [24], completely differed from the case and established that privacy is of persons and not places therefore privacy rights are maintained even in those information which are voluntarily revealed to a third party.

The increase in frequency of surveillance will have a direct effect on invasion of privacy. The menace from diluting the data protection laws in India will give major defense to the government. As pointed out by Justice Sanjay Kishan Kaul in K.S Puttaswamy judgement that “surveillance is not new, but technology has permitted surveillance in ways that are unimaginable [25]”. Even with the provision for warrant, courts give legal orders without proper scrutiny and with uncertainty about the legal safeguards against surveillance in this digital age.

Mass surveillance is based on technology structure which keeps the parameter of privacy protection at lowest or the government abuses the exception as a rule. For example, the government is trying to remove end to end encryption or to keep the length of encryption at low, it can be easily understood that such measures are to make easy access of data through surveillance. It is important to distinguish two types of surveillance based on whether it promotes democratic principles i.e., achieving power equalization in local government or it is exercised for security of the nation resulting in coercion and repression. Limitation imposed on individual autonomy should be removed for being against the essence of democracy.

Need For Redesigning India's Surveillance Law

How easily through mass surveillance privacy of a citizen can be violated, makes us think about re-evaluating and redesigning our privacy laws. In PUCL's case [27], the Court observed that telephonic data was an essential section of contemporary life" [28]. With the revolution in communication facilities in India, the Court noticed (to some degree interestingly from the present perspective) that there is an increase in frequency of people carrying mobile phones in their pockets".

The significant problem of a public authority’s mass projects of mass surveillance, including the Centralised Monitoring System, is that there is no particular legislation which backs up such mass surveillance. This is a risky issue for a key clarification - existing India’s law expects that inspection could be centered around. In People Union for Civil Liberty, the court characterized 'capture' under section 5(2) of the Indian Telegraph Act, 1885 similar to the interference of interchanges shipped off or from a particular location, and identifying with a particular individual, the two of which should be indicated in the block attempt request. This thought is rehashed by Rule 419-A63 similarly as the IT Act system [29]. It means that all the trades on telephone or IP systems can be checked but as there is no law on mass surveillance therefore it creates a vacuum providing no privacy protection to the victims.

Another serious issue with the current surveillance law system is that it provides abundance of power to the legislature. In the PUCL judgment, the court refused to make it a requirement of scrutiny by the judiciary for request by the government for interception of calls and gave this important task to the executive. This method should be reanalyzed for two main reasons. Firstly, it rejects the principle of separation of powers, and makes an irreconcilable situation within the executive division, which is liable for both the surveillance of a target individual, and to decide whether such interruption causes infringement in his personal space. With the basic rights of all the citizens at risk, which was seemingly not the situation when PUCL was concluded, it takes a higher priority than any time in recent memory that interception requests be independently assessed to decide if they are genuine enough to legitimize encroaching a citizen’s right to privacy. Second, as the last eighteen years have indicated that the PUCL rules are

inclined to being misused without any important ramification for the violator. This experience prompts the result that the expertise of the judiciary to have a check on the arbitrary interference in the privacy is a best method to protect privacy rights of the citizens. The judiciary can take grounds of "reasonable justification" to decide if a warrant should be allowed in a particular case or not.

Balancing The Right to Privacy with State's Interest

The ongoing tussle between an individual's right and power of state will continue because their interests do not align to each other though the real problem is whether state will limit its powers [30] and consider the value attached to an individual's privacy. There is a pressing need to create an equilibrium in their respective interests “balancing” is a term used in American Jurisprudence and refers to multi factor interest analysis [31] whereas in India in aadhar judgement, a proportionality test was ascertained. The states are easily invading privacy as if the government conducts targeted surveillance, it still has certain safeguards but if it is done without a proper warrant and any evidence is procured from it then it becomes admissible in court in India unlike in the U.S where such evidence becomes inadmissible.

To create a wall between such invasions we need a combination of legal reforms along with dialogue. The people need to consider whether their expectation of privacy aligns with how much privacy in reality is provided to them as many people would easily trade off their privacy and provide warrantless disclosure to the government. To create a dialogue among people, the government needs to provide more insight by creating transparency and promoting more media coverage on such topics. The greatest challenge in creating a balance is non-uniformity in laws which creates confusion and allows backdoor entry to the government agencies to invade privacy. The courts can play an effective part by providing careful scrutiny on a case-to-case basis and can provide external oversight to ensure that there is no abuse by surveillance systems.

Mass Surveillance raises the major concern in India, where CMS is getting opaquer since states can intercept communication directly without requesting telecom service providers. The courts can adopt a two- tiered approach where in case of an act which is adequately intrusive of an individual’s privacy should must be supported by a warrant backed by probable cause, while a lesser intrusion can have a reasonable suspicion. Additionally, courts should take on review of digital mass surveillance rather than reviewing individual acts of surveillance.

Conclusion And Suggestions

India is emerging as one of the biggest surveillance states and stands only after countries like Russia and China. The recent development of data privacy laws will be helpful to create a wall between the citizens and the companies due to the consent-based sharing but additionally it provides unrestrained powers to the central government which ultimately defeats the intent of the legislation. Data privacy has gained substantial importance during the times of the Covid-19 Pandemic as the world has changed its functioning and economies all around have adapted to the new regime of work from home. The governments across some states have exploited the individual’s right to privacy to fight the Pandemic. The compulsory implementation of Contact Tracing Apps across some states had given the state a loftier power to use and exploit an individual’s approach as and when it required. To fight such a regime, the approach should be two-faced. A scenario where the government implements stricter norms for I.S.P.s to have firewalls systems, deletion of data after the Pandemic is over, limit control of Internet of Things, and have users decide every aspect of access the IoTs have, will enable citizens to rely on and after that enjoy the right to privacy and personal information as well as sensitive personal information being protected.

The current Pandemic has facilitated a better data protection regime and improved right to privacy practice worldwide. It has made individuals analyse how essential data and information is. The practice of anonymity and imparting knowledge of hacks, intrusion, data robbery, cyber hacks, cybersecurity are rising, and the development of the same is to be welcomed as it is the future of the world’s economy.

Data gathering and Surveillance have a major impact on the privacy rights of an individual which is vastly misused by the governmental agencies on one side whereas the current legislation which protects individual data privacy also stands at a very weak place. One of the first steps towards creating a secure digital data platform is to make the people understand the value of their data and privacy as there is a lack of knowledge as to why such data should be protected and who the regulators are and how such regulations occur. The exception provided to the government to conduct mass surveillance should be looked into and if a situation demands internet surveillance, then it must be a targeted search with proper transparency and accountability of the agency. The right to conduct surveillance cannot be undermined in case of national security; therefore, a more balanced approach should be taken by only allowing state interception if there is reasonable evidence for such intrusion i.e. following the U.S model. The section 44 of

the IT act should be amended to include legal specifications for a request to extract information to minimize the potential for abuse. The role of the review committee is very essential to put checks on any arbitrary exercise on the part of the state. The decryption of data should be protected and will only be subject to inspection when such governmental agencies provide adequate amounts of evidence for its seizure.

References

[1] Bhatia G (2014), STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BIOGRAPHY, National Law School of India Review Vol. 26, No. 2 (2014), pp. 127-158, retrieved from https://www.jstor.org/stable/44283638?seq=1&cid=pdf accessed on 23rd October 2020.

[2] Padmanabhan A, Singh V (2019), The Aadhaar Verdict and the Surveillance Challenge, 15 INDIAN J. L. & TECH. 1, retrieved from http://home.heinonline.org accessed on 25th October 2020.

[3] Ramachandran C (2014), PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for the Digital Age, 7 NUJS L. REV. 105, retrieved from http://home.heinonline.org accessed on 26th October 2020.

[4] Chakraborty et al., Data Protection Laws Demystified (1st ed. Oakbridge Publishing Pvt. Ltd. 2019).

[5] Brazeal G (2020), Mass Seizure and Mass Search, 22 U. PA. J. Const. L. 1001, Retrieved from http://home.heinonline.org accessed on 22nd October 2020.

[6] Slobogin C, SURVEILLANCE AND FOURTH AMENDMENT, Privacy at Risk: The New Government Surveillance and the Fourth Amendment, ISBN: 9780226762944, University of Chicago press books, 2008, Retrieved from http://home.heinonline.org accessed on 27th October 2020.

[7] Foreign Intelligence Surveillance Act of 1978, Pub. L. 95–511, 92 Stat. 1797, 50 U.S.C, Retrieved from https://www.scopus.com/home.uri on 27th October 2020.

[8] Smith S. L. (2014), Abidor and House: Lost Opportunities to Sync the Border Search Doctrine with Today's Technology, 40 NEW ENG. J. oN CRIM. & CIV. CONFINEMENT 223, Retrieved from http://home.heinonline.org accessed on 22nd October 2020.

[9] Gliksberg C (2017), Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technologies, 50 Loy. L.A. L. Rev. 765, Retrieved from https://digitalcommons.lmu.edu/llr/vol50/iss4/7/ accessed on 25th October 2020.

[10] American Surveillance: Intelligence, Privacy, and the Fourth Amendment by Anthony Gregory. Madison: University of Wisconsin Press, 2016. xiii + 263 pp. Retrieved from http://home.heinonline.org accessed on 27th October 2020.

[11] K. S. Puttaswamy vs Union of India(2017) 10 SCC 1

[12] Kharak Singh vs State of Uttar Pradesh 1964 SCR (1) 332

[13] State vs Charulata Joshi 1996 (37) DRJ 445

[14] People's union for civil Liberty vs Union of India(1997) 1 SCC 301

[15] Nations D, What Does 'Web 2.0' Even Mean? How Web 2.0 Completely Changed Society, LIFEWIRE, Retrieved fromhttps://www.lifewire.com/what-is-web-2-0-p2-3486624 accessed on 7th December 2020

[16] Nield D, How to See Everything Your Browser Knows About You, GIZMODO,Retrieved from http://fieldguide.gizmodo.com/how-to-see-everything-yourbrowser-knows-about-you-1789550766 accessed on 8th December 2020 ; Geoff Duncan, 7 Ways Your Apps Put You at Risk, and What You Can Do About It, DIGEST TRENDS, Retrieved fromhttp://www.digitaltrends.com/mobile/seven-ways-apps-put-risk-cant-really accessed on 8th December 2020

[17] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors, W.P. (Civil) No. 494 of 2012

[18] MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY(Department of Information Technology)NOTIFICATION, 11th April, 2011 Retrieved from http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf accessed on 12th December 2020.

[19] Kessler D. J., Ross S ,Hickok Elonnai (2014), A Comparative analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation cross- border privacy rules, National Law School of Indian Review, Vol. 26, No. 1, pp. 31- 61, Retrieved from https://www.jstor.org/stable/i40179361 accessed on 10th December 2020.

[20] Id. at 22

[21] Munkaster P, India Introduces Central Monitoring System , The Register, 8-5-2013, retreived from https://www.theregister.com/2013/05/08/india_privacy_woes_central_monitoring_system/ accessed on 2nd December 2020

[22] Carpenter vs. United States, No. 16-402,585 U.S
[23] United States v. Miller, 425 U.S. 453
[24] Collector v. Canara, [10] 103 (2005) 1 SCC 4
[25] id. at 22
[26] Monahan, "Questioning Surveillance and Security," Retrieved from https://books.google.co.in/books/about/Surveillance_and_Security.html?id=YCg9QXSDAYYC&redir_esc=y accessed on 5th December 2020.
[27] id at 19
[28] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, 18
[29] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information), Rules, 2009, Rule 9.
[30] Teubner Gunther (2009), Self-subversive Justice: Contingency or Transcendence Formula of Law?, 72 Mod. L. Rev. 1, Retrieved from https://www.researchgate.net/publication/227584241_Self-subversive_Justice_Contingency_or_Transcendence_Formula_of_Law accessed on 20th November 2020.
[31] Solum Lawrence, Legal Theory Lexicon: Balancing Tests, Legal Theory Blog, retrieved from https://lsolum.typepad.com/legal_theory_lexicon/ accessed on November 23, 2020.