INVASION OF PRIVACY THROUGH SEARCH AND SEIZURE OF ELECTRONIC MEDIA: COMPARATIVE STUDY OF USA AND INDIA

Adv. Kshitij Bharat Gimhavanekar, B.A.LL.B, ILS Law College, Pune & LL.M,
Symbiosis Law College, Pune

ABSTRACT

Data has evolved much more important than oil as oil is a finite commodity whereas data has potential to grow at an exponential rate. With the recent development in the legal status of privacy, included as a part of fundamental right and with the drafting of the data protection bill 2019, the protection of data and privacy issues has gained major limelight. 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.

Keywords: Invasion, Technology, Privacy.

Chapter- I: 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. Technology strengthens the state to peek into the lives of the citizens and creates a large-scale privacy issue. The Right to privacy was recognized in the Puttaswamy judgment and it would be interesting to analyse its impact on instances of search conducted by the government agencies. After Puttaswamy judgement, the apex court has given legitimacy to the right to privacy and included it within the ambit of fundamental right under Article 21 of the Indian Constitution. There is a need to restore the balance and uphold individual rights, in this regard; the U.S model can be the inspiration we might look up for as it provides the protection of the fourth amendment. With the recent development on privacy rights, we have moved a step towards the U.S regime and hence we must also inspect the related developments in the U.S and other similar provisions to ensure a positive and smooth transition. 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". This amendment puts a check on the unregulated power of governmental agencies to conduct search and seizure and provides its citizens 'reasonable expectation of privacy.'

Statement of problem

Data Surveillance is a worldwide phenomenon throughout different geographies, economic development, and societal well being conducted by private and government entities. The framework of checks and balances of data protection dates back to 1996 which resulted in codification of rules in 2007 which permits only the Union Home secretary as a competent authority to issue an order for interception, monitoring and decryption. But, by authorizing other ten central agencies, the state is following the trajectory of a 'Surveillance State'. 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.

Research Questions/ Hypothesis

- With the advancement in technology, whether the outdated provisions related to Search and Seizure of electronic devices will be able to uphold the privacy rights of individuals?
- What is the role of the government in infringing privacy of its citizens?
- Whether Surveillance Laws in India needs to be re-designed?

Research Objectives

- To trace the journey of evolution of privacy laws from physical search to internet surveillance.
- To study about different parameters set for privacy by the Indian and USA laws.
- To understand the importance of reserving few powers to conduct surveillance cannot be undermined.
- To propose a system where accountability and responsibility of the government is to be increased with reasonable checks and balances
- To analyze the need of judicial scrutiny in the procedure of search and seizure.
- To access the need of strong legislation that protects individual privacy and community data.

Research Methodology

This is a doctrinal study where the researcher is trying to gain better insight into the provisions related to privacy rights and search and seizure, a comparative study was conducted of the laws in the USA and India. This research is based on literature already available hence the author further analyses the information to make an evolution of this research. This research involves secondary data such as books, articles, journals. Books on the subject, law journals, articles from various national and international journals, reports of committees, judicial pronouncements, All India Reporters, Supreme Court cases and etc. are the secondary sources of data for this research.

Scope & Limitation

There are a number of pressing issues surrounding state conducted surveillance that persist in our country. It was found during the literature survey that books related to privacy rights and

surveillance through electronic media was scantily available for India. Due to lack of knowledge and transparency, a common citizen does not recognize at what par he/she has privacy rights and who are the regulators and how such regulations occur.

Literature Review

The review has been aimed to analyze what has been done by other scholars and to identify the gaps in the research already done and to contribute towards filling the gaps left in the previous research.

Smith (2014) in Abidor and House: Lost Opportunities to Sync the Border Search Doctrine with Today's Technology[1]: The literature review shows that there has been a 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 being used to rationalize warrantless scrutiny of intimate digital documents and photos which has resulted in swallowing the rule itself." A person's digital life ought not to be hijacked simply 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 border agents must have "reasonable suspicion" that a device contains digital contraband before searching or seizing the device. Border search exception to the requirement of warrant applies only to routine searches, but searches of personal electronic devices are categorized into non-routine searches as it violates the first and fourth amendment.

Brazeal (2020) in MASS SEIZURE AND MASS SEARCH[2]: In light of the report regarding digital surveillance by the government, it is conceivable that the two-tiered system should be adopted to create a balance between an individual's privacy rights and the practical needs of governmental agencies. The author has created a link between two different cases which are: Carpenter v. United States and Teny v. Ohio where the former related to deeply the invasive

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

form of search using digital technology and the latter is minimally the invasive form of seizure "stop and frisk". The approach is that a digital search is corresponding to the two-tiered approach to the seizure of persons under Teny and if an act of digital surveillance is adequately invasive of an individual's privacy, the government must obtain a warrant backed by probable cause, but fewer invasion 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. However, following the same parameters for seizure and digital search will bring out arbitrariness as they are too far apart to be put on the same side of the coin.

Bhatia (2014) in STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BIOGRAPHY[3]:This paper begins with the evolution of privacy laws as per judicial interpretation in India, wherein Karak Singh case, personal liberty was grounded within the meaning of dignity, attaching it to the persons and not the places (the court still denied to expressly frame it, which was done in K.S Puttaswamy case) The court requires reasonable suspicion to authorize any search and anything more than targeted surveillance is ipso facto unreasonable. It is also reported in the article that the government must justify that the infringing laws are in the interest of the state and, it is infringing the right to privacy in the narrowest sense. This paper addresses the need for formal recognition of privacy laws, but yet there is no discussion on the admissibility of illegal evidence as a result of the unwarranted search.

Gliksberg (2016) in DECRYPTING THE FOURTH AMENDMENT: APPLYING FOURTH AMENDMENT PRINCIPLES TO EVOLVING PRIVACY EXPECTATIONS IN ENCRYPTION TECHNOLOGIES[4]: The literature review shows that encryption technology requires the backing of the grounds of the fourth amendment and regulating the backdoor entry of the government to access the data on the digital platform. The Government uses the third party exception to warrant requirement to access the data with the reasoning that the disclosure

[3] Gautam Bhatia (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.
[4] Candice Gliksberg (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.

to 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'. Applying the outdated legislation to the recent technologies is vague; the courts need to recognize the transformation the new digital technologies are bringing and give protection to encryption security under the fourth amendment as citizens have a reasonable expectation of privacy.

Padmanabhan & Singh (2019), THE AADHAAR VERDICT AND THE SURVEILLANCE CHALLENGE[5]: There have been numerous studies to discuss the landmark judgment of Aadhaar, but in this article, the focus is around the narrow interpretation of court regarding an individual's privacy rights. The court 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 favor 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 majority has ignored how State Resident Data Hubs (SRDHs) can be an easy tool for big data analytics and profiling. The legal system needs a sounder judicial model to access technological advancement and to have a holistic approach to protect privacy rights.

Slobogin in SURVEILLANCE AND FOURTH AMENDMENT from the book Privacy at Risk: The New Government Surveillance and the Fourth Amendment[6]: The literature review shows that surveillance can be divided into three parts: communication surveillance, physical surveillance, and transactional surveillance. Governments have long relied on all three types of spying. This e-book focuses on physical and transactional surveillance. The principal thesis of this book is that given their insult to privacy, autonomy, and anonymity, physical and transactional surveillance techniques must be regulated more extensively than they currently are. The fourth amendment prohibits unreasonable searches of "house, person, and effects". Relying on the American Supreme Court precedent that had for some time linked the definition of search to trespass doctrine in property law. In Terry vs. Ohio[7], the Supreme Court established a framework for analyzing the scope of fourth amendment protection towards the privacy of individuals. In particular, if the promise of Terry's case had been realized by the court the rules

[5] Ananth Padmanabhan & Vasudha Singh (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.
[6] Christopher Slobogin, 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] Terry v. Ohio, 392 U.S. 1, 13-14 (1968).

regulating physical and transactional surveillance would be more coherent and provide more protection of individual privacy.

Sculhofer in WIRETAPPING, EAVESDROPPING, AND THE INFORMATION AGE from the book MORE ESSENTIAL THAN EVER[8]: The Framers of the Fourth Amendment, In spite of the fact that acquainted with that training, picked language that awards protection just to "People, houses, papers and impacts" and requires court orders to determine "The things to be seized". Accordingly, when examiners in the mid-20th century went to wiretapping as law authorization instruments, sacred protection for private discussion was dubious. In Olmstead versus the United State Supreme Court held that an inquiry requires an actual interruption and that seizure happens just when the specialist takes material things become progressively delicate. In one case a government specialist entered a zone close to an office and set a mouthpiece against the divider so it intensified the connecting room. The court held that this was not pursuit on the grounds that there had no such actual section except for when the specialist utilized a "spike mike" that imagined the divider; the court held that that was search. That outcome left the Fourth Amendment of law Shambles, in light of the fact that the privacy of home was upset in a similar way.

The Katz decision was a major jump forward and not on the grounds that it stretched out sacred protection to wiretapping and expressed word. More significantly, Katz set out to settle the conventional brand of originalism that earlier courts had conjured to smother Fourth Amendment protection likewise in Katz choice The Supreme Court never scrutinized its holding that electronic eavesdropping of public telephone corners was restricted without warrant. The Fourth amendment plans to ensure each resident the occasion to guarantee everyday issues that can be offended from unhindered government spying. The designers considered such to be a possibly lethal treat to singular independence and political opportunity.

Gregory in THE FOURTH AMENDMENT MIRAGE from the book American Surveillance:[9] Modern technology appears to introduce both opportunities and threats that can change humanity qualitatively and forever. 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

[8] 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.
[9] 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.

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. 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. Randy Barnett and Jim Harper argue that the NSA bulk data collection program violates law and the fourth amendment. They are of the opinion that the Courts should not apply the doctrine of reasonable expectation of privacy rather it should adopt the traditional and reliable concept of property and contract rights. 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.

Ramachandra (2014), PUCL V. UNION OF INDIA REVISITED: WHY INDIA'S SURVEILLANCE LAW MUST BE REDESIGNED FOR THE DIGITAL AGE[10]: The literature 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 laws cannot keep up with the new digital age and surveillance projects deployed by the government. There is an urgent need for statutory backing to these projects and case to case review by the judiciary to create the balance between the executive and judiciary.

[10] Chaitanya Ramachandran (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.

Colin J. Bennett in his book, "The Privacy Advocates: Resisting the Spread of Surveillance"[11] has mentioned the rise of self-driven advocates to challenge the invasion of privacy through biometric systems, video surveillance and many others. He has gathered all relevant information through discussion and interviews with the people involved in the system. He addresses surveillance as a cause and privacy as a potential effect and fills an important gap in the previous available literature by understanding the rationale behind the resistance by the privacy advocates.

Chakraborty in his book Data Protection Laws Demystified[12] gives an insight into General Data Protection Regulation (GDPR) as it impacts transfer of personal data beyond the scope of the EU. It also discusses other regulatory areas, such as DNA technology, finance, and telecom, besides laws such as the Information Technology Act, 2000, and the Aadhaar Act, 2016.

Thematic Chapterization

The entire research work will run into six chapters. Chapter I: Introduction brings out the importance of the study and states its objective. Chapter II will discuss the privacy laws in India and the USA, its development. Chapter III will state about the globalization of technology and how search and seizure through electronic media are infringing the right to privacy. Chapter IV will discuss the need for re-designing India's surveillance laws, and Chapter V will be about balancing the right to privacy with the state's interest. Conclusion in Chapter VI followed by References.

Chapter- II: Development of privacy laws in India and the USA

There are several distinctive legal concepts within the privacy laws of the United States. Infringment of privacy, a tort based in common law which allows an aggrieved party to file a case against a person who illegally interrupts into their private matters, unveils their personal data, advances them in a wrong light, or uses their name to achieve something.[13] The quintessence of the law gets from a right to privacy, described generally as "the option to be not to mention." It as a rule bars individual issues or exercises which can likewise decently is of public interest, similar to those of VIPs or individuals in newsworthy occasions. Intrusion

[11] Bennett, Colin J (2008), The Privacy Advocates: Resisting the Spread of Surveillance, The MIT Press, JSTOR, Retrieved from www.jstor.org/stable/j.ctt5hhfb6 accessed on 12th December 2020
[12] Chakraborty et al., Data Protection Laws Demystified (1st ed. Oakbridge Publishing Pvt. Ltd. 2019).
[13] "Invasion of Privacy Law & Legal Definition", US Legal

of the privilege to privacy can be the preparation for a lawsuit for harm contrary to the individual or element disregarding the right. These incorporate the Fourth Amendment option to be liberated from inappropriate search or seizure, the First Amendment option to free gathering, and the Fourteenth Amendment fair treatment right, perceived by the Supreme Court as safeguarding a typical right to privacy inside family, marriage, parenthood, reproduction, and child raising.[14]

The improvement of privacy right started with English customary law which guaranteed "just the actual impedance of life and property". The Castle rule analogizes a person's home to their fortress – a site that is private and should not be open without assent of the owner. The improvement of wrongdoing fixes by the standard law is "one of the fundamental parts all through the whole presence of security law".[15] Those rights reached out to join "acknowledgment of man's otherworldly nature, of his sentiments and his intellect." Eventually, the extent of those rights widened significantly further to incorporate a fundamental "option to be not to mention," and the previous meaning of "property" would then contain "each type of ownership – theoretical, just as substantial." By the late nineteenth century, premium in privacy developed because of the development of print media, particularly papers.

The Personal Data Protection Bill, 2019, is on track with the privacy law in India that has been influenced by overall enhancements similarly as the country's own ensured law. The constitution of India doesn't explicitly make reference to privacy; but bridging the gap courts have held that an improvement to privacy laws under the light of fundamental right to life guaranteed under Article 21.[16] However, there was presence of some vagueness in every case regarding the particular idea of the confirmation of protection due to the long-standing judgment of the Supreme Court in Kharak Singh v. province of Uttar Pradesh, where the court held that protection to privacy cannot be granted as a fundamental right under the constitution.[17]

It became essential to decide this vagueness in view of two factors that ended up being dynamically appropriate: (1) shrill cases of loss of privacy in the wake of the government’s

[14] "Right to Privacy Law & Legal Definition", US Legal
[15] Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz (2006), Privacy, Information, and Technology, Aspen Publishers, pp. 9–11, ISBN 0-7355-6245-8
[16] Govind v. State of Madhya Pradesh AIR 1975 SC 1378; R. Rajagopal v. State of Tamil Nadu AIR 1995 SC 264; PUCL v. Union of India AIR 1991 SC 207.
[17] Kharak Singh v. state of Uttar Pradesh, AIR 1963 SC 1295

execution of its attempt for unique biometric recognizing evidence (Aadhaar)[18] and (2) overall development happening at the same time. The improvement of the Indian data innovation industry and the telecom change, which started in the last era of the 1990s, incited the development of automated organizations in India. This has had two tremendous results. To begin with, the nation is progressively interconnected because of the development of advanced administrations and stages. Second, the public authority has perceived that online assistance conveyance is an incredible vehicle for accomplishing strategy goals, for example, monetary consideration and conveying money moves. The resulting objective has been urged generally by the utilization of Aadhaar. In any case, the creating inescapability of Aadhaar went under upheld examination from various quarters. One analysis was that Aadhaar was being used for purposes other than social-government help transport, for instance, customer onboarding by private firms. It was stated that the limit of Aadhaar-related customer data, for instance, metadata about the spot of affirmation, established a serious breach of privacy.[19]

The European Union (EU) in 2013 proposed to consolidate its data protection structure through the General Data Protection Regulation (GDPR). The past structure was based upon the 1995 European Data Protection Directive for guaranteeing singular data. It was felt that this regulatory structure would provoke a separated arrangement of data affirmation inside the EU. The GDPR experienced wide adjustments of meetings lastly came into power in 2018. This work to make an intensive data affirmation rule in the EU influenced the conversation in India.

The discussion on the privacy issues in light of Aadhaar brought about a class of petitions under the watchful eye of the Supreme Court that tested the legitimacy of the enactment that empowered the framework: the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The five judged bench of the appex court heard the petitions and expressed that, since the petitions asserted encroachment of the right to privacy, it was first imperative to decide if such a right existed under the constitution. Later on this issue was referred to a bench of nine judges of the appex court in the year 2017, the court stated that a right to privacy can be granted under Article 21, that the appex court had chosen the inquiry mistakenly in Kharak Singh, and that enlightening privacy was a piece of this privilege to privacy. The Supreme Court's judgment signified a takeoff from before resolution on two

[18] "Users in India to Reach 627 Million in 2019," Economic Times, , Retrieved from **https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627 million-in-2019-report/articleshow/68288868.cms?from=mdr** accessed on November 23, 2020

[19] "Madhav Khosla and Ananth Padmanabhan, "The Aadhaar Challenge: 3 Features That Put Constitutional Rights at Risk,"

grounds. To begin with, it evidently and unambiguously communicated that there was a significant right to security under the constitution. With respect to this paper, in any case, the more enormous ground was that the advantage to security was conceptualized as an advantage in itself, free of what protection it guaranteed accordingly. In a long line of past cases, security was used to guarantee express interests, for instance, protection from night time police visits in the Kharak Singh case or security from telephone tapping in PUCL v. Association of India.[20] The Supreme Court's judgment in Puttaswamy rather conceptualized security as a correct worth ensuring in itself. This seemingly prompted a concentrate away from the genuine damage people would experience the ill effects of an infringement of security. Significantly, as clarified below, this conception of privacy also aligned with already existing regulatory frameworks in data protection in other jurisdictions.

Chapter- III: 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.[21] 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.[22]

This technological revolution is not 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

[20] PUCL v. Union of India, AIR 1963 SC 1295; and (1997) 1 SCC 301

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

[22] David Nield, 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 from http://www.digitaltrends.com/mobile/seven-ways-apps-put-risk-cant-really accessed on 8th December 2020

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 hit of pandemic, the world is now more relying 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 right to privacy as a fundamental right by the Supreme Court of India.[23] 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 InformationTechnology 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.[24] The rules states definition of personal data that it includes medical records, biometric information, passwords, financial data and sexual identification[25] 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 judgment of Aadhar.[26] The 2019 bill has given significance to consent and protects autonomy of an individual's data,

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

[24] 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.

[25] David J. Kessler, Sue Ross and Elonnai Hickok (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.

[26] Id. at 22

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 agency of U.S. and U.K uses extensive surveillance systems like PRISM and TEMPORA to spy on their own citizens, similar episodes are happening in India, Central Monitoring System (CMS) provides collection of telephonic data by tapping[27] 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 significant terrorist attack of 9/11 in the year 2001, USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to 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[28], 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,[29] 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

[27] P. Munkaster, 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
[28] Carpenter vs. United States, No. 16-402,585 U.S
[29] United States v. Miller, 425 U.S. 453

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,[30] 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 defence to the government. As pointed out by Justice Sanjay Kishan Kaul in K.S Puttaswamy judgment that “"surveillance is not new, but technology has permitted surveillance in ways that are unimaginable."[31] 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.[32] Limitation imposed on individual autonomy should be removed for being against the essence of democracy.

Chapter-IV: 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 re-designing our privacy laws. In PUCL's case,[33] the Court observed that telephonic data was an essential part of contemporary life, and were often of an intimate and confidential nature".[34] With the revolution in communication facilities in India, the Court noticed (to some degree interestingly from the present perspective) that "more and more people are carrying mobile telephone instruments in their pockets". If the PUCL Court were to talk

[30] Collector v. Canara, [10] 103 (2005) 1 SCC 4
[31] id. at 22
[32] 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.
[33] id at 19
[34] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, 18

today, it would positively discover contemporary types of correspondence (counting email, online media, VoIP, and Google look, among others) to be similarly meriting the Constitution's assurances of protection and opportunity of articulation. In order to provide an effective mechanism to protect these rights, there is a need to restructure current surveillance laws.

A significant problem of the public authority's mass surveillance projects, including the CMS, is that there is no particular legislation which backs up such mass surveillance. This is a risky issue for a key clarification - existing Indian law expects that inspection will be centered around. In PUCL , 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.[35] Nevertheless, the sort of inspection to be finished using the CMS turns this thought on its head - essentially all trades on the telephone and IP networks in India can be checked in a general plan. As existing law doesn't consider such a mass observation, it is as of now being finished in a lawful vacuum with no protections for resident's privacy rights. This is clear administrative overextend.[36]

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 to 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 person's right to privacy. Second, as the last eighteen years has indicated that the PUCL rules are inclined to being misused without any important ramification for the violator. This experience prompts to the result that the expertise of the judiciary to have a check on the

[35] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information), Rules, 2009, Rule 9.

[36] The Hindu, Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic, September 9, 2013, Retrieved from https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece accessed on 25th November 2020.

arbitrary interference in the privacy is a best method to protect privacy rights of the citizens. This judiciary can take ground of "reasonable justification" to decide if a warrant should be allowed in a given case.

Chapter V: Balancing the Right to privacy with state's interest

The 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[37] and consider the value attached to an individual's privacy. There is a pressing need to create a equilibrium in their respective interests “balancing” is a term used in American Jurisprudence and refers to multi factor interest analysis[38] 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 more opaque 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,

[37] Gunther Teubner (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.
[38] Lawrence Solum, Legal Theory Lexicon: Balancing Tests, Legal Theory Blog, Retrieved from https://lsolum.typepad.com/legal_theory_lexicon/ accessed on November 23, 2020.

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

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.

References

Books and Journal articles

1. 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.

2. Ananth Padmanabhan & Vasudha Singh (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. Candice Gliksberg (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.

4. Chaitanya Ramachandran (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.

5. Christopher Slobogin, 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.

6. Elle Xuemeng Wang (2019), ERECTING A PRIVACY WALL AGAINST TECHNOLOGICAL ADVANCEMENTS: THE FOURTH AMENDMENT IN THE POST CARPENTER ERA, Berkeley Technology Law Journal Volume 3 Issue 4, retrieved from https://doi.org/10.15779/Z385T3G08H accessed on 20th November 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. Gregory Brazeal (2020), Mass Seizure and Mass Search, 22 U. PA. J. Const. L. 1001, Retrieved from http://home.heinonline.org accessed on 22nd October 2020.

9. Gautam Bhatia (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.

10. Shannon L. Smith (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.

Online Websites

1. The Hindu, Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic, September 9, 2013, Retrieved from https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece accessed on 25th November 2020.

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

3. David Nield, 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

4. Geoff Duncan, 7 Ways Your Apps Put You at Risk, and What You Can Do About It, DIGEST TRENDS, Retrieved from http://www.digitaltrends.com/mobile/seven-ways-apps-put-risk-cant-really accessed on 8th December 2020