Page 1148 - 1159 **DOI:** http://doi.one/10.1732/IJLMH.25348

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 6

2020

Privacy and Surveillance: A Constitutional Conundrum of Essence of Right and Justification for its Denial

IRA KUMAR[1]

ABSTRACT

With the growing threats to national security, interest etc. often measures are adopted by the state to address these concerns by intercepting information, placing the privacy of citizens at a risk. While the technological revolution already continues to threaten people's privacy, surveillance further reduced the notion of 'privacy' to a myth.

This paper seeks to resolve the constitutional obfuscation of privacy as a constitutional right and surveillance by state as a reason for its breach. The paper first traces the evolution of the concept of privacy in India and in US, both jurisdictions where the constitutional right of privacy is a result of judicial construct. It then examines the essence of privacy as a right as it exists in India and the US by delving into the interpretation of 'privacy' and statutory provisions supporting privacy in both the jurisdictions. The paper analyses the conflict between surveillance and privacy by examining the surveillance laws in India and US. The paper highlights the existing judicial safeguards which if extended to all surveillance measures, create a model surveillance framework that serves the interest of national security perfectly and also limits the extent of surveillance to only that which is justifiable. The paper also examines the Personal Data Protection Bill,2019 and its potent role in reconciling privacy and surveillance.

I. INTRODUCTION

The concept of 'privacy' has evolved over the years with the varying values and degrees of self-realization among different societies. While there exists no fixed definition for this term, it is understood through facets of domestic privacy, physical privacy, communication privacy and lately even information privacy. The earliest perception of privacy was limited to domestic and physical privacy, and it was considered a privilege that guarded one's opinions, actions choices shared within their four walls as confidential. With the changing perceptions of the modern democracies, privacy evolved as one of the most fundamental liberties required

[1] Author is a student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

for a dignified human life.

The earliest attempts at defining the contours of privacy explain it as a right synonymous to the *"right to be left alone*".[2] This simple expression of the term highlighted the essence of privacy. With the growing political awakening and advancements in the society, this concept was extended to the realm of communications to prevent any unnecessary interventions in this realm of personal space. With the advancements in technology like the emergence of artificial intelligence, machine learning, Big Data, information communication technology etc. there are newer threats and challenges posed to the right to privacy in this digital age.

It cannot be disputed that privacy has emerged as one of the most important rights in any modern democracy. The international instruments of human rights like Universal Declaration of Human Rights[3], International Covenant on Civil and Political Rights[4] etc. have further established right to privacy as one of the most prominent human rights. Keeping up with this perception of privacy, nations have incorporated this protection in their Constitutions. For older Constitutions like that of US and India, the method of judicial construction has been relied on to read this right into the constitution.

(A) Statement of Problem

9/11 attacks, 26/11 Mumbai attacks, pandemic 2020 etc. have placed the national security and interests in a precarious state, forcing the governments to restore to surveillance to intercept "intel" to prevent any further harm to nations security or interests. However, the technological modernisation has made surveillance a threat to the privacy of individuals. This has sparked an international debate on the tussle between individual's right to privacy and state's need for surveillance. *While nations are still in the process of adopting legal frameworks ensuring protection for invasion of privacy, a legal gap is created by exempting the state from the scope of such frameworks to carry out surveillance under the pretext of laissez faire functions*. Not only does this pave way for misuse of wide surveillance powers by the executive, but it also devalues the spirit of constitution by placing national interests above civil liberties.

(B) Research question

Is the constitutional right of Privacy, as it exists today in India and USA, a myth or an achievable reality? What is the essence of the constitutional protection of privacy?

---

[2] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REV. 193 (1890)
[3] Universal Declaration of Human Rights, 1948, Art. 12.
[4] International Covenant on Civil and Political Rights,1966.

 [ISSN 2581-5369]

To what extent should the laissez faire pretext of surveillance measures be allowed to justify invasion of privacy? How can a balance be struck between national interest and civil liberty to uphold the spirit of constitutionalism?

(C) Research objectives

The article seeks to analyse the essence of privacy as a constitutional right through a comparative jurisprudential perspective to establish that the current state of legal privacy frameworks and the interpretation of privacy under these frameworks leaves it vulnerable to infringement, making privacy a myth. The article examines the constitutional obfuscation of surveillance and privacy to observe that unreasonably broad and sweeping measures for surveillance, invading the protected liberties of individuals, for the purpose of regulation of activities under state control, are not ideal for the spirit of constitutionalism in a democratic society.

II. FOUNDATION OF RIGHT TO PRIVACY IN THE US AND INDIA

(A) USA

In the Western Civilization, the evolution of privacy began as a consequence of awakening of self-realization among the people, a realization that a person's feelings, motivation etc. were most private to him[5] and that there existed a personal space within which no public intrusion was allowed by law.[6] It was the changing notion of sociability which led people to value a restricted private life centred around the individual and his family.[7] From being limited to domestic life the concept of privacy was extended to physical privacy owing to a newly developed understanding of individual autonomy and identity in the nineteenth century.[8] It was around this time that privacy began to gain acknowledgement as a legal right in the US.

Privacy under common law

Before being recognised as a constitutional right, privacy developed as a legal right under the common law. Two factors that profoundly contributed to the growth of common law right to privacy were the growth of press and technology. A new wave of journalism surfaced in the nineteenth century that banked on aggressive sensationalism for popular support and in doing so compromised much of America's privacy.[9] The technological advancements led by the

[5] Peter Brown, *Late Antiquity*, in I A HISTORY OF PRIVATE LIFE, 229,232 (Paul Veyne ed., 1987).
[6] Georges Duby, *Introduction*, in II A HISTORY OF PRIVATE LIFE, 6 (Georges Duby ed., 1987).
[7] Philippe Arias, Introduction, in III A HISTORY OF PRIVATE LIFE, 9 (Roger Chartier ed., 1987).
[8] Georges Duby and Philippe Braunstein, *The Emergence of the Individual*, in II A HISTORY OF PRIVATE LIFE, 511 (Georges Duby ed., 1987).
[9] George T. Rider, *The Pretensions of Journalism*, 135 N. AM. REV. 471, 478 (1882)

 [ISSN 2581-5369]

invention of telephones, instant camera, telegraph etc. pushed the media frenzy to intrude into the private lives of people more often.[10]

S. Warren and L. Brandeis in the work "The Right to Privacy" laid the foundation of the common law right of privacy by arguing that the common law guaranteed all individuals the right to decide the extent to which others should be communicated about their private thoughts and emotions.[11] By the end of the 20th century, many states had acknowledged privacy as a common law right.[12]

Privacy as a constitutional right

Although privacy has not been explicitly mentioned in the American Constitution, the spirit of individualism, personal liberty and limited government embedded in the Fourth Amendment has led to privacy being read into it. The Supreme Court has applauded the Fourth Amendment for being the soul of constitutional liberty, an essential for the enjoyment of the other fundamental rights.[13]

While the concept of privacy under the Fourth Amendment was earlier limited to the notion of "trespass" of homes, papers etc. (physical privacy), with the advent of communication systems, notion of privacy was extended to this realm as well. Where in *Olmstead v. United States*, the court was reluctant in relinquishing the "trespass doctrine" in favour of privacy[14], it was in *Katz v. United States* that the court taking a new approach devised the notion of "expectation of privacy". It observed that only those expectations of privacy of an individual would be protected under the law which are deemed to be "reasonable expectations" by the society.[15]

It was in *Griswold v. Connecticut*[16] that the court gave a new boost to the interpretation of privacy as a constitutional right by holding the law prohibiting contraceptives as unconstitutional for violating the privacy of married couples. It reasoned that even for government regulated acts, the state could not use intrude upon the privacy of people by employing unnecessary wide measures. Further in *Roe v. Wade* the court reading the right of an unmarried women to abort as her private choice held that some "*zones and areas of privacy*" are recognised by the courts, such notion of privacy originating from "*first, fourth*

[10] DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 67 (1978)
[11] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 198 (1890).
[12] William L. Prosser, Privacy, 48 CAL. L. REV. 386, 389 (1960).
[13] Gouled v. United States, 255 U.S. 298, 304 (1921)
[14] Olmstead v. United States, 277 U.S. 438.
[15] Katz v. United States, 389 U.S. 347, 359 (1967)
[16] Griswold v. Connecticut, 381 U.S. 479 (1965).

and fifth amendment, in the penumbras of Bill of Rights and the concept of liberty." [17]

(B) INDIA

The placement of privacy as a constitutional right is solely a matter of judicial construction.

In *M.P. Sharma v. Satish Chandra*[18], dealing with the issue of privacy in search and seizure cases for the first time, the court rejected the notion of privacy in such cases. In *Kharak Singh v. State of U.P.*, the court held night domiciliary visits to be violative of personal liberty. However, it refused to explicitly recognise right to privacy as a constitutional right.[19]

In *Gobind Singh v. State of Madhya Pradesh*[20], a case similar in context to Kharak Singh case, marked the onset of privacy law in Indian Constitution. While the court held the impugned law to be not violative of Art. 19 and 21, it stressed upon the importance of privacy as a right. The court in this case adopted the "compelling public interest" test, setting a higher standard of review of any law violating privacy under Art. 21. It also adopted the "narrow tailoring test" to ensure that any restrictions on privacy were structures as narrowly as possible.

This strong privacy protection standard adopted in Gobind case was applied to the *PUCL v. Union of India*[21] to hold that "*only rigorous standards can justify infringement of privacy*".

Finally, the latest case of *Justice K.S. Puttaswamy v. Union of India* re-established privacy as a fundamental right under the Constitution.[22]

III. CONSTITUTIONAL RIGHT TO PRIVACY: A MYTH OR AN ACHIEVABLE REALITY?

Tracing the development of right to privacy not only helps one understand the changing perceptions of the notion of privacy and but it also helps in examining the essence of right to privacy as it exists today in both jurisdictions of the US and India. Even though privacy has been read as a fundamental constitutional right in both the jurisdictions, it still continues to remain a distant dream.

While the US judiciary has read privacy in the spirit of the civil liberties guaranteed under the Constitution, it is the flexible conceptual approach to privacy that narrows the scope of the

[17] Richard Posner, *The Uncertain Protection of Privacy by the Supreme Court*, SUP. CT. REV. 173 (1979)
[18] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300.
[19] Kharak Singh v. State of U.P., A.I.R. 1963 S.C. 1295.
[20] Gobind Singh v. State of Madhya Pradesh, 1975 A.I.R. 1378.
[21] PUCL v. Union of India, (1997) 1 S.C.C. 301.
[22] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1.

 [ISSN 2581-5369]

term.[23] Privacy under the US jurisprudence is measured through the lens of "*expected privacy*". The protection against intrusion is guaranteed only where there is a "reasonable expectation of privacy". This test only affords protection to acts which are intended to be done in private as it is only reasonable to expect privacy in any place other than public spheres. This approach limits the extent of this protection and essentially eliminates privacy protection in today's age, where the modernisation of technology has made any "expectations of privacy" futile.[24] *Thus, despite having constitutional and legislative safeguards in place ensuring right to privacy, the narrow reading of the concept fails its purpose.*

While privacy in India is no new concept, but as compared to the US, the Indian evolution of privacy still remains in its nascent stage. While on one hand, US enforces the right to privacy through an abundance of legislations, India only acknowledges privacy based on the constitutional guarantee of privacy, a result of judicial construct. *Privacy even though recognised as a fundamental right, there is not bite to it in the absence of a privacy law setting into place adequate safeguards for its violation*.[25]

When privacy continues to remain a distant reality, new hurdles are posed by the technological advancements by raising the standards of expected privacy, which the laws are failing to keep up with. In an age where access to an individual's private life is a mere click away, surveillance has emerged as the most prominent threats to privacy. Functioning in a system void of any accountable checks, states have been adopting drastic surveillance measures concerning national interests and security with an implicit acceptance that these are reasons compelling enough to justify all unsought infringements of privacy of citizens.

This face off between surveillance for national security and right to privacy brings us to the dilemma that is compromising on the spirit of constitution the only way to win the battle against threats to national security. *Where on one hand the obligation lies on the state to protect any infringement of privacy as a fundamental right, does the same obligation not apply to the states when it is them breaching the individual privacy? To what extent is this breach justified under the excuse of national security?*

If the state is to truly honour the constitutional and international protection to privacy, a balanced approach rather than blatant invasion of privacy for national security has to be

[23] Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008)
[24] Andrew E. Taslitz, *The Fourth Amendment in twenty-first Century: Technology, Privacy and Human Emotions*, 65 LAW AND CONTEMPORARY PROBLEMS (2002)
[25] Agnidipto Tarafder, *Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA And India*, 57 JOURNAL OF THE INDIAN LAW INSTITUTE 550, 578 (2015)

 [ISSN 2581-5369]

adopted by bringing all surveillance measures under the scrutiny of law. This balanced approach entails defining what exactly is meant by "privacy" and its breach, "security" and "surveillance". This can be achieved by prescribing what information is required to be collected for surveillance, situations which make surveillance a justified necessity, method of carrying out such surveillance measures with an independent body to authorise and check all invasions of privacy by such measures.

IV. SURVEILLANCE V. PRIVACY

The era of surveillance did not just end with the World Wars but was revived with a renewed vigour post the 9/11 attacks which disturbed the US Homeland Security to the core. From the 2013 Edward Snowden revelation which shook the world sparked the conflict between privacy and surveillance for national security at an international level. *Which weighs heavier- national security or citizen's right to privacy has since remained the most contested question.*

Increasing instances of use of surveillance techniques to further political agendas have added to the fire by raising questions on the extend of justifiability of invasion of individual sphere under the pretext of security. In India, the introduction of Aadhaar as a welfare move invited much concern over privacy issues associated with the ease of surveillance that Aadhaar made possible.[26] The recent uncertainty surrounding the Aarogya Setu app developed as a surveillance measure during pandemic has further raised privacy concerns.[27]

Recently a PIL has been filed against the surveillance systems of CMS, NATGRID and NETRA, measures tracking all telecommunications in India, as "threats to privacy"[28]. It remains to be seen who trumps in this conflict between security and privacy.

These growing concerns for privacy bring us to the question that to what extent can the laissez-faire pretext of surveillance be used by the states to justify infringement of citizen's fundamental right to privacy.

(A) Surveillance Laws in US and India

The Patriot Act of 2011 is the leading and the most contested surveillance legislations of US. With the fresh memories' of 9/11 attacks, charged political atmosphere, pressure from the

[26] Kathryn Henne, *Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India*, in INFORMATION, TECHNOLOGY AND CONTROL IN A CHANGING WORLD (HAGGART B., HENNE K., TUSIKOV N. eds., 2019)

[27] *CIC slams NIC, MeitY for evasive reply on Aarogya Setu app, issues notice*, INDIAN EXPRESS, (December 8, 2020, 12:30 PM), https://indianexpress.com/article/india/aarogya-setu-national-informatics-centre-nic-government-statement-69

[28] *High Court seeks Centre's stand on PIL against NETRA, NATGRID surveillance systems*, THE ECONOMIC TIMES, (December 8, 2020, 12:30 PM), https://economictimes.indiatimes.com/news/politics-and-nation/high-court-seeks-centres-stand-on-pil-against-netra-natgrid-surveillance-systems/articleshow/79525462.cms

public and the helplessness of the legal authorities, the Congress was forced to bring in this Act which allowed for a greater scope of functioning to the intelligence bodies, which they earlier could not owing to the limitations set by civil liberties.[29]With the broadened scope of surveillance, the concern for the constitutional guarantee of privacy took the backseat.

The earliest surveillance laws of India include the Indian Telegraph Act, which deals with the monitoring of calls in cases of "public emergencies" or "public safety" and the Information Technology Act, which allows for the surveillance of data by government in certain cases. Both these laws regulate the domain of communication surveillance in India.

Post the *PUCL v. Union of India*[30] judgement, where the court held that where the law authorising interception of communication was backed by existence of "*adequate procedural safeguards*", invasion of privacy resulting from interception under such law was not violative of constitutional guarantee. In the absence of any statutory safeguards for guiding such interception, the court laid down interim guidelines which were later adopted as Rule 419A in the Telegraph Rules, 2007 and Rules u/S 69, 69B of the IT Act in 2009[31].

A review of these communication surveillance Acts revealed the many inconsistencies in them, which the statutory safeguards were not able to address owing to their non-transparent and unaccountable nature, making the misuse of such surveillance measures easier without providing the individuals any adequate remedy.[32]

26/11 attacks promoted for the adoption of more intelligence infrastructures.[33] The Centralised Monitoring System (CMS) allowed the collection and monitoring of telephonic data, WhatsApp and e-mails. NETRA, was a "dragnet surveillance system" designed to monitor the Internet traffic for words like "bomb", "blast", "attacks" etc. NATGRID surveillance system kept a track of bank details, travel itinerary, visa and immigration details etc.

As per the latest PIL filed in the Delhi High Court against these surveillance systems, it is asserted that the large number of authorisations being granted for monitoring individual's travel details and financial records under the garb of public interest amounted to a gross

[29] *supra* note 19.
[30] PUCL v. Union of India, (1997) 1 S.C.C. 301
[31] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[32] *Report of the Group of Experts on Privacy (*2016), PLANNING COMMISSION OF INDIA, 7: 19, 60, 61, (December 7, 2020, 10:00 AM), http:// planningcommission.nic.in/reports/genrep/rep_privacy.pdf
[33] Sharad Vyas, *Big leap in intelligence infrastructure post 26/11*, THE HINDU, (December 7, 2020, 10:00 AM), https://www.thehindu.com/news/national/big-leap-in-intelligence-infrastructure-post-2611/article25600377.ece

 [ISSN 2581-5369]

violation of privacy, even after there being safeguard measures in place.[34]

(B) Judicial Safeguards of Necessity, Proportionality and Legitimate state action

In the celebrated case of Justice Puttaswamy v. Union of India, the court dealt with the question if there existed a constitutional protection for privacy. The court read privacy as indispensable to live a "life of dignity and liberty" and held that privacy was in fact a *"constitutionally protected right which emerged from guarantee of life and personal liberty under Art. 21 of the constitution".*[35]

The court further observed that right to privacy under Art. 21 was not absolute. As long as any law infringing upon the constitutional right of privacy presented a "*fair, just and reasonable procedure*", it would not be invalid. It laid down a three-step test to determine if an infringement of privacy was justified. First was ***the test of legality***, which *"postulates the existence of law to justify the encroachment on privacy*". Second was ***the test of necessity*** which defined the "*aim of the state to ensure that law does not suffer from manifest arbitrariness*" and third test was that of ***proportionality***, which looked into "*the rationale nexus between the objects and means to achieve them"* to prevent any arbitrary invasion of privacy.

Instead of allowing the state complete exemption for infringement of privacy under the pretext of national security or welfare measures, *all state surveillance measures should be subjected to the checks of "necessity", "proportionality" and "legality" to justify the encroachment on privacy and to justify that the state surveillance measures are not arbitrary.*

Earlier, in *Gobind v. State of Madhya Pradesh*[36], the court had devised the "compelling public interest" and "narrow tailoring" test to set a check on the infringement of privacy under Art. 21. The "compelling public interest" test reflected on the higher degree of check established for privacy under Art. 21 than other freedoms under Art. 19. The "narrow tailoring" test also an US test mentioned in the case of *Grutter v. Bollinger*[37]provided that any state action infringing upon the right of privacy should be framed such that privacy is invaded in the narrowest possible way while fulfilling the state aim behind such invasion.

These tests envisioned by the judiciary and read by them into the constitutional right of privacy reflect on the expected standard of protection of privacy to be followed by all contested laws. The implications of these checks of either the "*compelling public interest*"

[34] *supra* note 22.
[35] Justice K. S. Puttaswamy and Ors. v. Union of India, A.I.R. 2017 S.C. 4161.
[36] Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148.
[37] Grutter v. Bollinger, 539 US 306, 333 (2003)

 [ISSN 2581-5369]

test or "*narrow tailoring*" test, or of the test of "*legality, necessity and proportionality*" on the state surveillance instruments shows that the state must be able to illustrate ***why a certain category of data or information is required to be intercepted and monitored*** and ***whether the extent of the surveillance for the purpose of public interest or security is as narrowly structured as possible so as to infringe the fundamental right of privacy as per the "narrow tailoring" test***.

It remains to be seen how the CMS, Netra and Natgrid surveillance systems, in the latest PIL by Centre for Public Interest Litigation, employed for wide surveillance in India are read into the existing surveillance laws to stand these tests to justify the broad nature of surveillance on communication, financial and other personal information of individuals.

While these systems can be read into the existing surveillance laws to justify their purpose, the existing surveillance laws still fail to provide for a remedy if these surveillance measures are held violative of the fundamental right of privacy. This is why a new sound legal framework is required which establishes a provision for remedy in case of infringement of privacy, especially by surveillance measures.

(C) Personal Data Protection Bill, 2019: A misguided beacon of hope for India?

The Personal Data Protection Bill, 2019 is an example of how states instead of correcting the legal lacunas are more inclined towards reducing them. While this much awaited privacy legislation is expected to extend the protection of privacy from a mere constitutional guarantee read by judiciary to a statutory protection as well, it still fails to establish a stringent legislative framework for privacy.

For a country where about 1.3 billion people are left exposed to the constant monitoring by the state surveillance systems, the issue of surveillance and its impact on fundamental right of privacy becomes pertinent, especially when the state laws are failing to keep up with the technological modernisation. The Personal Data Protection Bill, 2019 could have been the guiding light out of this tussle by establishing a balance between surveillance and privacy. However, the Bill fails to address this conflict.

Personal Data Protection Bill has given the state carte blanche power to conduct surveillance by exempting the government from the scope of the Bill under the pretext of "*national security, integrity and sovereignty, public order, friendly foreign relations and preventing cognizable offence"*. These wide and undefined terms in the Bill make its application ambiguous, leaving it prone to misuse under these broad pretexts as is deemed fit by the

government.[38]

The government only needs to furnish a reasoned written order in order to claim its protection from the application of the Data Protection law, thus limiting the possible checks on this exercise of power by the executive. No provision of a judicial review is provided under the Bill to keep a check on the executive abuse of this power, thus making this framework a weak protection against mass surveillance.

V. CONCLUSION

The modernisation of technology has made the invasion of personal sphere easier, thus increasing the instances of privacy infringement. This makes the issue of protection of privacy, a right deemed as an essential, inherent human right, required to live a dignified life with liberty, important.

The right to privacy is the most threatened by the unbridled acceptance that the "need" to collect and monitor information for national security or other welfare reasons is a compelling justification to invade the sacred sphere of privacy. It is not disputed that the states need access to data for carrying out a number of its functions. However, a balanced approach is recommended between surveillance and privacy to prevent unreasonable and arbitrary surveillance by the state.

The pretext of a laissez faire state action is no more a good enough justification for the compromise of right to privacy of individuals. State has to be subjected to the same protection checks as are other private entities, and only a just, fair and reasonable breach of privacy should be allowed. A complete exemption from accountability and transparency devalues the spirit of the constitutional right of privacy, reducing privacy to a myth.

TOWARDS REALISING THE DREAM OF PRIVACY

A. ***A Robust Legal Framework:*** There is an urgent need for a robust legal framework guarantying protection for the constitutional right to privacy and laying safeguards for its breach with remedies for the aggrieved. Personal Data Protection Bill, 2019 is a step towards the light.

B. ***An Independent Review Body:*** Because surveillance for national interest, security etc. are left to the government, there is a need for a system of check to review that this power is not abused by the executive. A judicial or parliamentary body may be appointed to look over the

[38] *Personal Data Protection Bill, 2019: Recommendations to the Joint Parliamentary Committee, ORF Special Report No. 102*, OBSERVER RESEARCH FOUNDATION, (December 8, 2020, 10:00 AM), https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/

monitoring orders issued under the surveillance laws to limit surveillance to lawful and just needs only.

C. ***Safeguards for the intercepted data:*** While it is understood that in this data-driven world, data is required by the state for a number of reasons, the large amount of data intercepted is vulnerable to breach if not handled properly. Safeguards must be adopted for handling the data gathered through surveillance by ensuring adoption of proper encryption methods, thus balancing both surveillance and privacy.

D. ***Accountability of Intelligence Agencies:*** The existing surveillance law provides no penalties for abuse of power by the intelligence agencies and enforcement bodies. Accountability of such agencies should be enhanced by subjecting them to the same standards of protection of privacy as the private entities, in cases of breach. Accountability also encourages transparency in the surveillance systems.

E. ***Educating the Masses:*** Privacy is often viewed as an accessory of the privileged society. Especially in India, people fail to realise the indispensability of right to privacy for a dignified life. No law can succeed in ensuring protection against privacy unless people are aware about why they need such protection in the first place. It becomes important to educate the people to help them beware of their rights and to uphold the spirit of democracy.

*****

 [ISSN 2581-5369]