Jagannath University Research Journal (JURJ)

Volume No.-V - , Issue No. I, Month, April, Year, 2024 ISSN: 2582-6263

JURISPRUDENTIAL APPROACH TO PELLUCID PRIVACY LAWS IN THE DIGITAL AGE

Nityash Solanki[a], Prof. Shyam PalSinghShekhawat[b]

[a]110, Officers Campus Colony, Janak Marg, Jaipur – 302012, [b]NH-12, Tonk Road, Jaipur - 303901, Rajasthan

Abstract: Confidentiality of data shared by individuals, corporations and government on the Internet has become vulnerable to various cyber security threats. Privacy related legal regimes are under constant consideration in the Parliament of various States to combat issues related to data protection. The jurisprudence of privacy laws encountered significant attraction of philosophers, thinkers, and even political parties since the subject matter reached areas of government record management, health system, educational policies, banking and finance services. In the digital age, attempts have been made to extend the meaning of the term 'privacy' to include the right to control flow of digital data/information. Data protection laws can be found under numerous statutory rules and regulations implemented by States around the globe. However, the aim of these legislatively implemented privacy law suffers due to constant technological innovations and authorized government surveillance over digital personal data. It would not be incorrect to state that the trans-global nature of Internet has given rise to problems of 'privacy' in the information age. United Nations has instructed States to consider existing examples of International approaches to combat issues of data protection through appropriate legislations. In this paper, significant sources of data protection laws suggested/recommended by United Nations member States will be discussed to comprehensively evaluate the success rate of constitutionally implemented privacy laws on the cyberspace. This article makes an attempt to provide prospective jurisprudential approach to make suggestions for shielding digital age human rights and internationally accepted privacy regimes.

Keywords: Physical Privacy; Informational Privacy; Decisional Privacy; Proprietary Privacy; Associational Privacy; Intellectual Privacy.

~~the European Union drafted an "omnibus" data~~

I. INTRODUCTION

The origin of privacy laws can be traced back to 19th century when common law States approached to resolve issues related to the confidentiality and publicity through appropriate legislative regimes. Major statutes such as, The Electronic Communication Privacy Act of 1986 (ECPA); The Russian Federal Law on Personal Data (No. 152-FZ), 2006; French Data Protection Act, 1978; Data Protection Act, 2018; were enacted to resolve most recognized problems of digital privacy by some of the developed nations in the world. Digital Privacy laws gained political and social attention especially when intruders stole voluminous data, which become a threat to national security. The jurisprudence of privacy laws encountered significant attraction of philosophers, writers, thinkers and political parties since the subject matter reached government record management, health system, educational policies, banking and financial services.[1] It is worthy to note that interaction of Internet with telecommunication industry paved way for discussions in the United Nations over data protection rights. Consequently, protection framework that introduced privacy laws as a new branch of international human right. The most significant data protection legislation in the European Union is the "GDPR" i.e. "General Data Protection Regulation" (EU) 2016/679. It took no time for States to adopt a practical approach to examine cultural and traditional norms for framing privacy laws in their respective jurisdiction and beyond.[2] Common law States faced numerous ethical, philosophical and political controversies/debates before declaring privacy laws as an international human right. In this paper, components of information technology laws will be examined from the prospective of traditional notion of privacy. The global battle to tame the present digital era has opened a door way to elusive, vague and conceptual confusion contributing to lack of rigor regarding information privacy.[3] The contents of this paper will assist readers to identify crucial issues related to personal data protection often encountered by individuals, corporate giants and

[1] Edward Bloustein, Privacy as an Aspect of Human Dignity: An answer to Dean Prosser 39 New York University Law Review, 962 (1967); available at https://heinonline.org/HOL/LandingPage?handle=hein.journals/nylr39&div=71&id=&page=; accessed on 22nd April 2024.

[2] Daniel Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622; accessed on 20th April 2024.

[3] W. A. Parent, Privacy, Morality and the Law, Wiley, Vol. 12, No. 4 (Autumn, 1983), Philosophy and Public Affairs, pp. 269-288; available at https://www.jstor.org/stable/2265374; accessed on 20th April 2024.

government in the digital age. The global economy demands significant reconsiderations of legislative policies that revolve around invasion of privacy on the Internet.

II. COMPETING IDEOLOGIES

The 'freedom of speech' and 'right to privacy' meets the cross border of philosophical controversies in the digital age. In our opinion, the interaction of the two rights highlighted above has triggered policy makers to legislatively respond to the need of the hour by framing regulations for embracing the freedom of information age. Elision of information privacy law by States has promoted debates on international platforms over expansion of 'right to control data' and 'right to manage information flow'. For instance, the US Senate constantly questions corporate giants and social media platform such as Facebook, Twitter and Google to monitor and control the content that is posted on their respective social media platforms. As a matter of fact, there is a loop hole in the regulatory regimes to sue these corporate giants for spread of misinformation or bad user behavior since no statutory provisions are framed to legally bring 'a check and balance' system into place for moderating content posed by Internet users on social media platforms. Under such circumstances, the official representatives of these companies' takes the plea of being treated as a 'neutral middleman' just like newspaper seller instead of newspaper editors, who holds authority to moderate content or one who decides what goes into printing and what is to be left out. Furthermore, Section 230 of the Communications Decency Act, 1996 (CDA) creates a shield around companies from liability for hosting misinformation and misleading content uploaded on their websites by Internet users. It is pertinent to note that Section 230 of the CDA removes the protective shield of no liability for companies in cases where contents of information suggests serious criminal offences including child pornography or breach of Intellectual Property. Nonetheless, Section 230 has largely facilitated Internet companies such as Facebook, Twitter, Instagram, Youtube, Google, and many more to explore the ambits of 'freedom of expression' in creating Internet free speech as it know it today.[4] Therefore, citizens have become conscious to address the ethical and legal implication of digital communication surveillance.[5] Nevertheless, legit surveillance of Internet activities forms the basis of data protection laws for many States.[6] Breach of confidentiality either by intruders or sometimes authorized personals gives rise to privacy torts. The constitutional scheme that safeguards individual rights such as trade, religion, profession, marriage, lifestyle, reproduction, personal decision making, etc. has been unduly influenced by problems of law enforcement, national security and data surveillance activities by States. Regulating social media and journalism that promotes trans-border data flows is the key challenge for policy makers. This article makes an attempt to provide prospective jurisprudential suggestions to shield human rights and international privacy laws. Privacy laws framed by developed nations include international human rights perspectives.[7] Consequently, analysis of such regimes would form the basis of opinions and suggestions recommended for the information age through this article.

III. THE CONCEPT OF "PRIVACY"

A simple explanation of the term privacy could be understood by the phrase 'the right to be let alone'.[8] In the digital age, the meaning of the term has been extended to include 'the right to control flow of digital information'.[9] In legal parlance, the ambit of

[4] British Broadcasting Corporation, Facebook, Twitter, Google face questions from US senators, 28th October 2020, available at https://www.bbc.com/news/technology-54721023; accessed on 22nd April 2024.

[5] Howard B. Radest, The Public and the Private: An American Fairy Tale, The University of Chicago Press, Vol. 89, No. 3, Ethics (Apr., 1979), pp. 280-291; available at ; accessed on 20th April 2024.

[6] Simon G. Davies, Re-Engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity, Technology and Privacy: the New Landscape 143, 153 (eds., Philip E. Agre & Marc Rotenberg 1997); available at https://dl.acm.org/doi/10.5555/275283.275289; accessed on 20th April 2024.

[7] Stanley I. Benn, Privacy, Freedom and Respect for Persons, Nomos VIII: Privacy, Rputledge, (eds. J. Roland Pennock & John W. Chapman, 1971); available at Stanley I. Benn, Privacy, Freedom and Respect for Persons, Nomos VIII: Privacy (eds. J. Roland Pennock & John W. Chapman, 1971); accessed on 22nd April 2024.

[8] Alan P. Bates, Privacy – A Useful Concept? Social Forces, Vol.42, No. 4 (May, 1964), pp. 429-434; available at https://www.jstor.org/stable/2574986, accessed on 20th April 2024.

[9] Anita L. Allen, Presidential Address, "The Philosophy of Privacy and Digital Life," 93 Proceedings of the American Philosophical Association 21-38 (2019); available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4022657; accessed on 20th April 2024.

privacy is further stretched for two reasons; *firstly*, to safeguard integrity of information shared on digital platforms; and *secondly*, to facilitate conditional accessibility of data flow through legislative principles. In any event, the legal discourse on privacy laws in many States falls short of dichotomizing public and private information. Thus, privacy is a generic concept the precise definition of which is rather difficult to identify. Furthermore, research on the subject matter reveals six layers within which 'privacy' principles are embodied.[10] Prospective invasion of these layers by intruders would most probably give rise to appropriate legal actions before established law courts or adjudicating authorities in any given State. The social dimension of privacy nearly about four decades back was much smaller then what it is today.[11] For instance, lawyers, a few decades ago, strategically contended judge made laws to claim privacy rights to secure relief for their clients.[12] Professional organizations never miss a chance to harvest privacy promoting rules and regulations to boast their ticket to paradise at the market place. Theorists promote liberal interpretations to examine the ambit of privacy for high-tech data protection and security.[13] Civil libertarians advocates free speech and right to privacy against government's staunch intrusions in day-to-day affairs of citizens to assert freedom of information age. However, a purely legal prospective would identify the concept of privacy as freedom from most direct forms of illegitimate intrusions or constraints of any kind whatsoever.[14] The legitimate purpose of the concept of privacy under any given law for the time being in force is to encourage citizens to make conscious decisions and choices in their private life.[15] Factors that form six layers for the concept of privacy can be explained as follows:

3.1. PHYSICAL PRIVACY

Physical privacy is breached when somebody unlawfully peeks into other people's business for personal benefit or for mere pleasure.[16] For instance, a person named 'A' installs a secret camera or flies a drone over the dwelling house of a person named 'B' to record activities conducted behind closed doors. In this hypothetical scenario, A's conduct has breached the physical norms of secrecy, which is culturally marked as the highest level of privacy breach. Since dwelling houses are considered to be the heart of private life of its resident individuals, A's act would give a right to B for initiating an action in tort or a criminal action of trespass or for voyeuristic pleasure derived by A for spying on B. The act of installing cameras and flying drones over property disrupts the intimate seclusion of B and his/her family members from strangers. The layer of physical privacy emerges from the right to enjoy solitude in territorial or spatial boundaries of privately owned property.[17] Thus, the law makes it transparent that it is vital for a person to explore physical privacy, bodily integrity and territorial enjoyment of privately owned property.

3.2. INFORMATIONAL PRIVACY

[10] W. A. Parent, Privacy, Morality and the Law, Philosophy and Public Affairs, Vol. 12 No. 4, (Autumn, 1983), pp. 269-288; available at https://www.jstor.org/stable/2265374; accessed on 22nd April 2024.

[11] Ferdinand D. Schoeman, Philosophical dimensions of Privacy: An Anthology, Cambridge University Press, (December 2009); available at https://www.cambridge.org/core/books/philosophical-dimensions-of-privacy/0261E242C29A3A7B4942AD083A41A671; accessed on 20th April 2024.

[12] Adam D. Moore, Privacy Rights: Moral and Legal Foundations, Penn State University Press (2010); available at https://www.jstor.org/stable/10.5325/j.ctv14gp5q4; accessed on 20th April 2024.

[13] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, New York University Press (2004); available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131; accessed on 22nd April 2024.

[14] Adam D. Moore, Information Ethics: Privacy, Property and Power, University of Washington Press (2013); available at https://www.jstor.org/stable/j.ctvcwns7f; accessed on 20th April 2024.

[15] Alan F. Westin, Privacy and Freedom, American Bar Association, Vol. 22, No. 1 (OCTOBER, 1969), pp. 101-106; available at https://www.jstor.org/stable/40708684; accessed on 20th April 2024.

[16] Ferdinand Schoeman, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, (30th November 1984); available at https://books.google.co.in/books/about/Philosophical_Dimensions_of_Privacy.html?id=q_FrmXyl3hUC&redir_esc=y; accessed on 22nd April 2024.

[17] Patricia Boling, Privacy and the Politics of Intimate Life, Ithaca, N.Y. and London: Cornell University Press (1996); available at https://www.jstor.org/stable/3175660; accessed on 22nd April 2024.

The informational dimension of privacy requires legitimate purpose for peeping into data retained on work related computer devices.[18] Let us consider the ambit of informational privacy with a hypothetical situation. A curious corporate manager namely 'X', installs a software bug to replicate and read personal emails of his/her employee named 'Y' without any legitimate reason. Many corporate companies lawfully access work-related information even from personal devices of employees. However, such intrusions by industry employers are regulated by strict legislative norms to prevent individuals from fraudulent acts. In any event, X by installing software bugs to access content of employee's personal emails for illegitimate purposes breached the moral codes of informational privacy. X's conduct would most probably give rise to legal actions for breach of contract especially the confidentiality clause of Y's employment agreement. Thus, informational secrecy, data encryption and data protection forms the three pillars of informational privacy. Informational privacy safeguards individuals from unnecessary outside intrusions by ensuring legitimate control over sharing of personal information on digital computer devices. Developed nations have strategically framed regulations under appropriate provisions of law by limiting the duration to retain employees' personal information. Therefore, it is vital for employers to adhere to the principles of fair business practices to dodge legal actions for illegitimate breach of employees' informational privacy.

3.3. DECISIONAL PRIVACY

The overwhelming debate of decisional privacy has ambushed customs and traditions of religious groups in many States. Cultural practices based on religious beliefs are constantly intruded by government policies. The subject matter of decisional privacy is the most controversial layer of privacy norms.[19] Decisional privacy triggers situation of law and order especially due to lack of strategic response by policy makers and government. Decisional privacy touches almost every corner stone of statutory regimes.[20] When religious debates are not addressed diplomatically, the layer of decisional privacy could undercut the entire democratic structure of the State. Decisional privacy can be differentiated into categories:

a) PURER DECISIONAL PRIVACY: attracts legitimate intrusions by appropriate authorities since some decisions made in the private life by an individual would have a social impact on the entire society. Exempli gratia, a person named 'A' commits adult incest by alluring a close family member for personal benefits. Here, 'A' commits a crime that will most likely attract criminal statutory consequences. Furthermore, let us imagine that a person named 'A' decides to weaned off the ventilator switch for his/her family member namely 'B', who is in a vegetative state and is undergoing essential medical treatments. Consequently, if A is an India citizen, then his purer decisional privacy would be evaluated from the prospective of "*parens patriae* role" adopted by the courts in Aruna Shanbaug case. Denial by statutory norm related to individual's decisional privacy in the above mentioned hypothetical scenarios would provide impetus control to interfere in individual's decisional privacy.

b) VILER DECISIONAL PRIVACY: includes subject matter that is trivial in nature. For instance, a college student named 'X' decides to colour his/her hair electric blue or chooses a Chubchik hairstyle to attract attention or wears bonkers attire. X's decision, although weird, would merely harm privacy norms of any individual. Furthermore, X conducts in the above scenarios does not in any manner whatsoever disrupt social order. In any event, some readers would disagree with the statement made above given the fact that recently the Chief Minister of Rajasthan introduced a proper dress code to enter government offices during duty hours.

[18] Neil Richards, The Information Privacy Law Project, Georgetown Law Journal, Vol. 94, p. 1087, 2006; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=941181; accessed on 20th April 2024.

[19] Gleen Negley, Philosophical Views on the Value of Privacy, Law and Contemporary Problems, Vol.31 No. 2, Privacy (Spring, 1966) pp. 319-325; available at https://www.jstor.org/stable/1190674; accessed on 22nd April 2024.

[20] *Ibid*.

Nonetheless, the trivial acts of citizens of such nature remain uncontroversial in the eyes of privacy laws.

3.4. PROPRIETARY PRIVACY

Proprietary privacy is breached when intruders without the permission of actual owners of proprietary property such as photographs makes uses of the property as if it belongs to them.[21] For instance, a person named 'X' uses a landscape photographs clicked by Mr. 'B' to promote company's brand or if 'X' uses social security number/aadhaar number that belongs to Mrs. 'B' for personal gains at the market place illustrates loss of proprietary privacy of Mr. B. Because X involved himself in the unlawful act of identity theft, B could initiate legal proceedings in law court against X under the relevant data protection and identify theft acts. In everyday parlance, invasion of proprietary privacy includes attempts and acts of stealing personal identity, computer dialect, likeness, and information related to somebody's DNA/medical profile. Legislative regimes around the globe have pursued these acts of 'identity thefts' with appropriate statutory provisions. Nonetheless, general public still remains vulnerable to acts of identity thefts by intruders on the Internet. Rules and regulations regarding notions of proprietary privacy fall short of safeguarding confidential information stored on computer devices in the virtual world. Therefore, proprietary privacy styles certain acts of identity thefts by intruders as privacy concerns. In the U.S., President Obama directed the Department of Homeland security to initiate a sixty (60) days National Cybersecurity Awareness Campaign to inform industries, communities, academia, international partners, federal and state government regarding the threats of cyber security by proposing a model, namely, "STOP. THINK. CONNECT" for securing a trustworthy digital communication network in the country.

3.5. ASSOCIATIONAL PRIVACY

As the name itself suggests, associational privacy is invaded through seeking membership or access to an exclusive club of closed group.[22] The agenda of meetings at such exclusive club includes discussions over subject matter related to politics, financial, social, civil, religious or cultural discussions. Exempli gratia, a person named 'A' seeks for a membership in an exclusive club with agenda to discuss religious norms. A receives the membership by dishonestly representing himself as belonging to the same religious orientation that is shared by other members of the group in that exclusive club. The manager of the club 'B' does a background check to confirm A's religious orientation and concludes that A is unworthy to become elite member of the exclusive club. Furthermore, the club members demands resignation of membership from A since he lacks the elementary understanding of the religious group's agenda. Discrimination of this kind may provoke unsettling feelings to persons discarded to become members at exclusive clubs. In the above illustration, A may or may not be held liable under statutory norms; however, A conduct of seeking membership on false pretences could invoke regulatory actions from the manager in charge of the religious group. Thus, seeking participation in closed religious groups invades associational privacy of individuals. Theorists and philosophers back associational privacy on the basis of the rhetoric of ancient privacy norms. In other words, association of individuals belonging to similar thoughts or orientation could assert restriction to shut out people with different religious orientation, sexuality, race, caste, etc. Therefore, it is pertinent to note that foundations of associational privacy is based on strong believes of physical, informational, financial, and decisional privacy.

3.6. INTELLECTUAL PRIVACY

Intellectual privacy safeguards a standard pattern of mental repose.[23] It is worthy to note that think tanks and intellectual members of our society actively participate to organize venues to

[21] Judith W. DeCrew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, Cornell University Press (1997); available at https://www.jstor.org/stable/10.7591/j.ctv75d3zc; accessed on 22nd April 2024.

[22] Anita L. Allen, Privacy, Encyclopedia of Privacy (William G. Staples, ed., Greenwood 2007); available at https://scholarship.law.upenn.edu/faculty_scholarship/2291/; accessed on 20th April 2024.

[23] Neil Richards, Intellectual Privacy, 87 Texas Law Review 387 (2008); available at https://texaslawreview.org/wp-content/uploads/2015/08/Slobogin-87-TLRSA-25.pdf; accessed on 20th April 2024.

transform/promote pious deeds to the world. Such intellectuals restrict individuals with forbidden thoughts to break the sanctity of thoughtful discussions over innovation for the 'progress of science and art'. Intellectual privacy demands a watchdog scheme to protect intimate knowledge of innovators, writers, musicians, and artists. Intellectual privacy aims to ascertain integrity of thoughts to engineer and capitalize on state of the art technology brought into existence by great innovators. For instance, a person named 'X' enters at the gathering of intellectual individuals of society and depicts images of innovative homemade pornography to disrupt gracious discussions of creative works of laureate physicists. Intrusions of X in the above hypothetical apparently disturb noble price wining physicists. Moreover, X's intrusion would result into unwanted confusions in the mind of intellectuals of any given State resulting into dichotomizing citizens into lower and higher groups by government. Intellectual privacy evokes notions of freedom to produce goods and services that ultimately enables the State to capitalize innovations. Therefore, upholding the norms of mental repose must be included as an agenda in legislative regimes to protect intellectual think tanks especially for promoting the progress of science and art in any given State.

IV. COMPREHENDING PURELY PRIVATE SPACE IN THE INFORMATION AGE

The private sphere of information can be legitimately classified into variety of distinctions based on factors such as: (a) public and private; (b) governmental and non-governmental; (c) official and unofficial; (d) open and secret; (e) societal and individual; (f) communal and personal; (g) *res publicae* (matters of community) and *res privatae* (individual and family matters); (h) polis and oikos.[24] An individual's right to privacy is construed as sacrosanct in the digital age. In law, however, the moral construct of privacy is walled-off from direct or indirect government regulations.[25] For instance, a person's choice to marry somebody falls within the domain of private sphere and is not interfered per se by the government. In any event, the government requires the couple to be mature for making the decision to marry by imposing age restrictions. Furthermore, legal provisions are framed to authenticate marriages by lawfully registration of marriages. Therefore, it would not be incorrect to state that modern state fails to consider the impervious boundaries of private activities of individuals for social, political and economic welfare. Modern states are prompted to intrude into privacy through surveillance over personal identity, freedom of speech and expression and other related private spheres of individuals' life. To justify these surveillances the modern state takes the plea of preserving rule of law, social values and practices.[26] The essence of surveillance is to protect freedom of expression, personal identity, reputation, integrity, dignity etc. of individuals from unlawful threats.

V. CRITICAL ANALYSIS OF 'DPDP' AND DOMESTIC USE OF CYBERSPACE

In India, The Digital Personal Data Protection Act, 2023, (hereinafter the "DPDP Act") was introduced as a watchdog scheme to protect personal data belonging to an individual. The DPDP Act incorporated essential provisions for process personal data of an individual for lawful purposes. Section 2(t) and Section 2(u) defines personal data and personal data breach. Personal data under the DPDP Act is equated with personal identity, in other words, information that is sufficient to identify an individual. As far as, personal data breach is concerned, it is defined as intrusion into personal data that alters or destroy the confidentiality and integrity of personal information belonging to an individual. It is pertinent to note that a loop hole in the DPDP Act is created under Section 3(c) since processing of personal data by an individual especially for domestic purposes is kept out of the loop of protection. In the digital age, most individuals connect to the Internet platform to avail the benefits of goods and services that are available in the cyberspace.

[24] Howard B. Radest, The Public and the Private: An American Fairy Tale, University of Chicago Press, Vol. 89, No. 3 (Apr., 1979), pp. 280-291; available at https://www.jstor.org/stable/2380076; accessed on 22nd April 2024.

[25] Jurgen Habermas, The Structural Transformation of the Public Sphere: An inquiry into a category of bourgeois society, Cambridge, Mass: MIT Press, 1989; available at https://archive.org/details/structuraltransf0000unse/page/n1/mode/2up; accessed on 22nd April 2024.

[26] Beate Roessler and Dorota Mokrosinska, The Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge University Press (2015); available at https://books.google.co.in/books/about/Social_Dimensions_of_Privacy.html?id=Dxy_CQAAQBAJ&redir_esc=y; accessed on 22th April 2024.

VI. JUSTIFICATION FOR DOMESTIC PRIVACY RIGHTS

By excluding processing of personal data for domestic purposes the DPDP Act has exposed individuals to face the vulnerabilities of cyber security at one's own risk. This grey area of the DPDP Act demands for a Parliamentary discussion over purely individualistic choices and efficient legislative regimes to counter cyber security threats. We do not deny that participation on social media comes with certain responsibilities; however, the democratic structure of our community motivates us to engage in healthy discussions to express opinions though Internet expressions. Consequently, legislative strategies for safeguarding the psychological well-being of individuals on social media platforms are required. It is highly recommended that the obligations of Data Fiduciary for the purposes highlighted under Chapter II of the DPDP Act must be extended to incorporate statutory regimes to process personal data processing by an individual for domestic purposes as well. Thus, Data Fiduciary could be given the responsibilities to monitoring legitimate use of personal data shared by an individual either for domestic purposes or on social media platforms. For instance, if a person named 'X' uploads his/her personal data while blogging views on social media and it turns out that the uploaded information is used for unlawful purposes, personal gains or annoyance. Under such circumstances, X should be assisted through a statutory provision for initiating a complaint with Data Fiduciary especially to guard psychological well-being of 'X' from unwanted attempts by intruders that causes nuisance to X. There could be two ways to approach such issues; *firstly*, Data Fiduciary could issue a notice to the social media website/platform to take down the personal information shared by X from the blog post; secondly, Data Fiduciary could assist X by sending a show cause notice to the social media website/platform to explain the wrongdoing. Furthermore, Section 6(1) of the DPDP Act requires restructuring to adjudicate instances highlighted in the hypothetical situation illustrated above. The sharing of personal data by individuals for domestic and social media purposes remains ambiguous under the DPDP Act. Thus, opportunities to exercise the constitutional right to freedom of speech and expression are unreasonably curtailed by the obstructive nature of DPDP Act. In our opinion, Section 3(c) of the DPDP Act hints towards a totalitarian approach taken by the 'majority of the elected members' of Parliament that perspicuously defeats the present liberal democratic requirements of the digital era. The ambits of cyberspace are infinite and individuals are eager to explore venues of capitalistic economy on the Internet. The recent privatization of various industries in India also suggests framing of statutory safeguards under DPDP Act to combat the vulnerabilities of sharing personal data by individuals for domestic purposes. As a result, Section 6(1) of the DPDP Act related to consent by the Data Principal requires restructuring to include instances of cyber security vulnerabilities especially when Data Principal shares personal information for specified/legitimate domestic purposes.

VII. CONCLUSION

In India, a legit prospective to "the right to privacy" was mandated by the Apex court by the judgment laid down in Justice K.S. Puttaswamy (Retired). v. Union of India and Ors.[27] Constitutional analysis of Article 21 by the Apex Court in the above stated judgment extended the common law reasoning to explain essential features of "right to privacy". The judgment delved into fundamental analysis of Article 21 of the Indian Constitution and the findings of the court scrutinized 'balancing tests' to bring forth the correct statutory interpretation of Article 21 and accorded "the right to privacy" to citizens of the country. Parliamentary intent and true purpose of Article 21 that provided citizens of India "the right to privacy" and "data protection" was made possible by the Apex Court through precedent based application of privacy laws in common law jurisdictions. A thorough consideration of judgment reveals extensive demand by libertarians for change in frontiers of political and philosophical surrounding of India. Practical application of privacy laws in day-to-day life clearly demands identifications of reasonable/balancing factors between segregationists and integrationists. Thus, it would not be incorrect to state that the foundation of Citizenship (Amendment) Act, 2019 for implementing the structure of social integration was lawfully construed by the court through interest-balancing between segregationists and integrationists. The skirmish protects surrounding The Citizenship (Amendment) Act, 2019 in the capital region of India proved to be a double edged sword for the Apex Court since judiciary was requested to examine cultural controversies/wars and interest-balancing of racial segregation. Thereafter, the exponentially growth of privacy

[27] **(2017) 10 SCC 1.**

laws in India reached the status of legal practice in its own right. At present, the global battle to tame the digital era has opened a door way to elusive, vague and conceptual confusion contributing to lack of rigor regarding information privacy in many States. Advocates are motivated to gather knowledge of privacy laws since the newly introduced right frequently demands understanding of interrelationship of privacy laws with civil liberties, health, civil rights, criminal laws, intellectual property laws, banking laws, etc. The legislative history of common law States reveals that legal reasoning and policy-making analysis demands extensive research into cultural and traditional surrounding of civilized society. An individual's right to privacy is construed as sacrosanct in the digital age. Nonetheless, opportunities to exercise the constitutional right to freedom of speech and expression are unreasonably curtailed by the obstructive nature of DPDP Act. As stated in the preceding portions of this article, the recent privatization of industries in India for facilitating 'the ease of doing business' demands framing of statutory safeguards under the DPDP Act to combat cyber security vulnerabilities in relation to sharing of personal data by individuals especially for domestic purposes. Thus, policy makers are prompted to intrude into domestic privacy issues kept out of the ambit of DPDP Act by adopting strategic surveillance schemes. Areas such as personal identity, freedom of speech and expression and other related private spheres of individuals' life need protection under DPDP Act to reinforce rule of law, social values and legitimate Internet practices for the digital era. We recommend the law makers of our county to create competent authority entrusted with the duty to monitor Internet free speech. The essence of surveillance by competent authorities so created under the proposed amendments to DPDP Act should be made responsible to preserve freedom of expression, personal identity, reputation, integrity, and dignity of individuals from unlawful cyber security threats.

ACKNOWLEDGEMENTS

It gives me immense pleasure to present this paper on the jurisprudential aspects of privacy law in the digital era. I extend warm regards to my family who helped, assisted, supported and encouraged me to research on privacy law statutory regimes and its long-term socio-economic impact on our society. I continue to gratefully recognize the contribution and support of my Ph.D. guide Prof. (Dr.) S.P.S. Shekhawat, who motivated me to continue the study on the subject-matter of the presented paper. I could not have done it without his contribution and support. I gratefully acknowledge and appreciate the working knowledge of Prof. (Dr.) S.P.S. Shekhawat, who has always enlightened me to achieve the set target within time.

REFERENCES

[1]. Edward Bloustein, Privacy as an Aspect of Human Dignity: An answer to Dean Prosser 39 New York University Law Review, 962 (1967).
[2]. Daniel Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006.
[3]. W. A. Parent, Privacy, Morality and the Law, Wiley, Vol. 12, No. 4 (Autumn, 1983), Philosophy and Public Affairs, pp. 269-288.
[4]. British Broadcasting Corporation, Facebook, Twitter, Google face questions from US senators, 28th October 2020.
[5]. Howard B. Radest, The Public and the Private: An American Fairy Tale, The University of Chicago Press, Vol. 89, No. 3, Ethics (Apr., 1979), pp. 280-291.
[6]. Simon G. Davies, Re-Engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity, Technology and Privacy: the New Landscape 143, 153 (eds., Philip E. Agre & Marc Rotenberg 1997).
[7]. Stanley I. Benn, Privacy, Freedom and Respect for Persons, Nomos VIII: Privacy, Rputledge, (eds. J. Roland Pennock & John W. Chapman, 1971); available at Stanley I. Benn, Privacy, Freedom and Respect for Persons, Nomos VIII: Privacy (eds. J. Roland Pennock & John W. Chapman, 1971).
[8]. Alan P. Bates, Privacy – A Useful Concept? Social Forces, Vol. 42, No. 4 (May, 1964), pp. 429-434.
[9]. Anita L. Allen, Presidential Address, "The Philosophy of Privacy and Digital Life," 93 Proceedings of the American Philosophical Association 21-38 (2019).
[10]. W. A. Parent, Privacy, Morality and the Law, Philosophy and Public Affairs, Vol. 12 No. 4, (Autumn, 1983), pp. 269-288..
[11]. Ferdinand D. Schoeman, Philosophical dimensions of Privacy: An Anthology, Cambridge University Press, (December 2009).
[12]. Adam D. Moore, Privacy Rights: Moral and Legal Foundations, Penn State University Press (2010).
[13]. Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, New York University Press (2004).
[14]. Adam D. Moore, Information Ethics: Privacy, Property and Power, University of Washington Press (2013).
[15]. Alan F. Westin, Privacy and Freedom, American Bar Association, Vol. 22, No. 1 (OCTOBER, 1969), pp. 101-106.
[16]. Ferdinand Schoeman, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, (30th November 1984).
[17]. Patricia Boling, Privacy and the Politics of Intimate Life, Ithaca, N.Y. and London: Cornell University Press (1996).
[18]. Neil Richards, The Information Privacy Law Project, Georgetown Law Journal, Vol. 94, p. 1087, 2006.

[19]. Gleen Negley, Philosophical Views on the Value of Privacy, Law and Contemporary Problems, Vol.31 No. 2, Privacy (Spring, 1966) pp. 319-325.
[20]. Judith W. DeCrew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, Cornell University Press (1997).
[21]. Anita L. Allen, Privacy, Encyclopedia of Privacy (William G. Staples, ed., Greenwood 2007).
[22]. Neil Richards, Intellectual Privacy, 87 Texas Law Review 387 (2008).
[23]. Howard B. Radest, The Public and the Private: An American Fairy Tale, University of Chicago Press, Vol. 89, No. 3 (Apr., 1979), pp. 280-291.
[24]. Jurgen Habermas, The Structural Transformation of the Public Sphere: An inquiry into a category of bourgeois society, Cambridge, Mass: MIT Press, 1989.
[25]. Beate Roessler and Dorota Mokrosinska, The Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge University Press (2015).

AUTHOR'S BIOGRAPHIES

AUTHOR'S BIOGRAPHIES

First Author: Mr. Nityash Solanki has an impressive academic background. He holds dual LL.M. degrees from The George Washington University and The University of Manchester, specializing in Intellectual Property Law and International Business & Commercial Law. At present, he is pursuing Ph.D. degree in the field of "Cyber Law". The testament for his passion for continuous learning skills adds to his dynamic personality. His extensive experience includes serving as State Government Standing Counsel for RSMM Department in the Rajasthan High Court from 2019 to 2022. With over twelve years of diverse legal experience, Nityash brings invaluable expertise in handling complex legal issues and litigating skilfully. His four conference publications include paper titled "Legal Aid in India: Returning Philosophical Chords", BRICS Law Journal Volume 11 (2015) Issue 2 via presentation on Professional Identity and Formation Workshop organized by Holloran Centre for Ethics and Leadership, St Thomas School of Law; and 2nd Conference of the European Network for Clinical Legal Education (ENCLE) in conjunction with 12th IJCLE conference, OLOMOUC (Czech Republic). He has more than 14 publications out of which 9 are in renowned SCOPUS (Q1, Q2 listed journals) and UGC Care I listed journals.

Second Author Prof. S.P.S. Shekhawat, is a knowledge think tank in the field of academics. He was formerly appointed as Dean, Faculty of Law at University of Rajasthan .He secured a toppers position at University during his LL.M. program. At present, he is appointed as Head & Dean, Faculty of Law at Jagannath University, Jaipur. His supervisory role as guide for more than twenty Ph.D. candidates proved fruitful in suggesting legislative policies to Parliament. His dynamic personality is built upon renowned positions held such as; Journal Editor of Journal of Legal Studies Editorial Board; Chairman at National seminars; Expert Member of Academic Board at Indian Law Institute, New Delhi; Expert Member of selection board at R.P.S.C., Ajmer. He enlightened various judges, academicians and young scholars by publishing almost around forty research papers in prestigious Journals on emerging legal issues including; uniform civil code, sustainable development, Human Rights, Constitutional laws, Judicial Activism, Mohammadan laws, Domestic Violence, Legal Aid, DNA profiling, Right to Information, Evidence Act, Rights of under trial prisoners.