IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 24, Issue 4, Ser. 7 (April. 2019) 57-63
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Critically Appraising the Personal Data Protection Bill, 2018

Karam Pratap Singh[1], Vaibhav Uniyal[2], Satarupa Datta[3],
Anna Anu Priya[4], Rahul Kumar[5]

[1](B.A. LL.B., V[th] Year, Law College Dehradun, Uttaranchal University, India)
[2](Assistant Professor, Law College Dehradun, Uttaranchal University, India)
[3](B.A. LL.B., IV[th] Year, Law College Dehradun, Uttaranchal University, India)
[4](B.A. LL.B., III[rd] Year, Law College Dehradun, Uttaranchal University, India)
[5](B.A. LL.B., II[nd] Year, Law College Dehradun, Uttaranchal University, India)
Corresponding Author:Karam Pratap Singh

Abstract: Data has become the most powerful thing in the world. People's personal life, their behaviour, politics, even sensitive issues like terrorism are touched by data. The only way to stop data - or those who control data - from controlling the entire human race is to guard people's right to privacy and bring together data protection laws. India is a nation with more than 1.25 billion people, all of whom are data-principals sharing their data with one data-fiduciary or the other. It has more than half billion internet users - now that internet is cheaper than ever - several startups have mushroomed, and given that India is the world's second largest market after China, the right to privacy and data-protection laws have become a necessity. Projects like Digital India, Make in India, and other technology and data-driven projects only make data protection even more important. This is something which even the apex court has acknowledged in Puttaswamy. The Sri Krishna Committee was given the task to create a framework for data protection law in India, after much deliberation, efforts of the committee showed up in form of the Personal Data Protection Bill, 2018. The Bill has comprehensively laid down the data protection scheme which includes - Data Protection Obligation; Grounds for processing of Personal Data or Sensitive Personal Data or Data of Children, Right of Data Principals; Transparency and Accountability Measures; Transfer of Personal Data outside India; Exemptions; Data Protection Authority of India; Appellate Tribunal and a host of other provisions, this paper critiques the Bill.

Keywords: Data, Data Protection, Privacy

Date of Submission: 04-04-2019 Date of acceptance: 19-04-2019

I. INTRODUCTION

"To avoid criticism say nothing, do nothing, be nothing." **— Elbert Hubbard**. This Article analyses the Personal Data Protection Bill, 2018, and critically evaluates the Bill on several counts - harm-based approach, data ownership, consent, categorization of data, government exemption, processing of data of children, right to be forgotten, data breach notification, authorities under the Bill, surveillance reforms, inter alia.

II. CRITICAL APPRAISAL OF THE PERSONAL DATA PROTECTION BILL, 2018

A. Harm Based Approach - The Bill has adopted a harm[1] based approach in defending data-principals from lapses by data-fiduciaries in treating their personal data. Whether in cases of grievances, notification of data breach, or adjudication under the Bill by the adjudicating officer, harm acts as a key determinant in deciding the course of action under the bill. Data principals have to approach the data-fiduciaries when harm is caused or there is the likelihood of it being caused in terms of the definition provided in Section 2(21) resulting from contravention of the provisions of the Bill by the fiduciary. The definition of 'harm' in the Bill inter alia includes – bodily or mental injury; financial loss; loss of reputation; loss of employment; fear of being observed or surveilled and any observation or surveillance not reasonably expected by the data principal. For seeking redressal, however, the data principal is burdened with the liability to prove harm which may not be possible to prove in all cases. Harm may not always manifest in quantifiable and measurable factors as evident from its

[1] The Personal Data Protection Bill, 2013, s. 2(21)

definition which includes elements such as mental injury, loss of reputation and fear of being observed or surveilled. The burden of proving such harm may have the effect of deterring data principals from actually reporting violations. The definition of harm does not contain a clause for violation of privacy and seeks to define the term through an exhaustive list leaving minimal scope for the definition to be dynamic and to incorporate changing technologies. The Bill should rather adopt a right based approach.

B. Data Ownership - According to the Bill, "data" - "means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means[2], "Data fiduciary" - "means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data"[3], and "Data principal" - "means the natural person to whom the personal data referred to in subclause (28) relates".[4] Further, person "means— (i) an individual, (ii) a Hindu undivided family, (iii) a company, (iv) a firm, (v) an association of persons or a body of individuals, whether incorporated or not, (vi) the State, and (vii) every artificial juridical person, not falling within any of the preceding subclauses"[5]. In the Bill, 'Data Principal' has been defined as a natural person whose personal data is in question whereas 'Data Fiduciary' is a person or entity collecting and processing that data. The Bill has not specified who will be the owner of the data. The Draft Bill completely steers clear from mentioning or acknowledging as to who owns such data. Perhaps one of the most critiqued miss from the Draft Bill, non-attribution of the ownership raises questions in relation to the effectivity of the Draft Bill.

C. Consent & Notice to Data Principal - Bill casts a duty on the data fiduciary to notify the data principal or to seek his consent "in a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable" at the time of collection of personal data.[6] In case of sensitive personal data, the notice includes information on granularity thus allowing data principals to access services without necessarily consenting to all or nothing. This enables the data principal to choose which data to share or to not share at all. However, such is not the case with personal data, here the data principal only has the option either to consent to share data or stop using the service. This is because of the unwarranted categorization of data into personal data and sensitive personal data. Granular control may be extended to personal data too. Data which are essential and necessary to deliver certain end-results (such as collection of location data for a navigation tool) may continue to be mandatory but for non-essential data, users should have control over its collection (such as access to a microphone for a navigation tool).[7]

D. Categorization of Personal Data - The Bill also establishes distinct standards for dealing with personal and sensitive personal data of the data principals. These standards should rather be uniform and not based on different categories of personal data. This is important given that the sensitivity of data is quite relative and modern data aggregation technologies are capable of revealing sensitive information from the processing of seemingly non-sensitive personal data.[8] Even outwardly anonymized data can be used to re-identify people, as shown by researchers from the University of Texas, who used anonymized data set released by Netflix and showed that it is possible to re-identify a Netflix user from the data set.[9]

E. Government Exemption & Non-Consensual Processing of Personal Data – The Bill lays down certain exceptions[10] that are widely worded in stark contradiction of the *Puttaswamy* judgment permitting the state to invade into privacy without seeking the consent of the data principal. These exceptions do not incorporate the test of 'Proportionality and Legitimacy' as laid down in *Puttaswamy* a.k.a. the privacy judgment for the invasion of privacy by the State. Sections 13(1) states that – "Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature". The Bill does not defines what "*function of Parliament or any State Legislature*" means. Similarly, the Bill has also not defined "service or benefit" in Section 13(2) and exempts obtaining of consent from data principals where the State under the law is providing such service or benefit. Same is the case with Section 19 which deals with sensitive personal data.

[2] The Personal Data Protection Bill, 2013, s. 2(12)
[3] *Id., s.2(13)*
[4] *Id., s.* 2(14)
[5] *Id., s.*2(28)
[6] *Id., s.8*
[7] Our Comments to the Draft Personal Data Protection Bill, 2018 to Meity, *available at*: https://privacy.sflc.in/our-comments-draft-data-protection-bill/ (last visited on March 6, 2019)
[8] Dvara Research: Response to white paper on data protection, *available at:* https://www.dvara.com/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf (Last visited on March 6, 2019)
[9] Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (Last visited on March 6, 2019)
[10] Supra note 2, ss. 13, 19

Both provisions 13(1) and (2) use the word "necessary", while Section 19 employs the phrase "*strictly necessary"* but no safeguards are provided to prevent misuse or abuse of such power given to the State.

F. Processing of Personal & Sensitive Personal Data of Children - The Bill has recognized children as a vulnerable group in need of a higher standard of protection. It contains a provision for processing of personal data and sensitive personal data of children.[11] The Bill enjoins a duty upon data fiduciaries to "process personal data of children in a manner that protects and advances the rights and best interests of the child."[12] The Section also devices a mechanism for age verification and parental control to be incorporated by the data fiduciaries for processing of personal data of children. The Bill, as it stands, does not adequately illuminate as to the mode of seeking parental consent and verifying age to protect children and their data. How parental consent will be obtained and how the age of a child will be verified are still areas that need research both at technological and legal fronts. However, the age verification mechanism should be in consonance with the principles of data protection and privacy, and should not infringe upon the rights of freedom of speech and expression of the children.

G. Right to be Forgotten - Section 27 of the Bill states "data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal"[13] where such disclosure "(a) has served the purpose for which it was made or is no longer necessary; (b) was made on the basis of consent under section 12 and such consent has since been withdrawn; or (c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature." This right is only exercisable if the Adjudicating Officer so determines and "the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen."[14] The section also provides that while determining the application of Section 27(2), the Adjudicating Officer shall have regard to "(a) the sensitivity of the personal data; (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life; (d) the relevance of the personal data to the public; and (e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented."[15] The right can be exercised "by filing an application in such form and manner as may be prescribed."[16] The section has also provided a mechanism for review under which - "where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2) does not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (3)."[17]

H. Personal Data Breach Notification -The Bill mandates that "the data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal."[18] There is no provision for notification to the data principal about breach of his personal data. Clause 5 of Section 32 of the Bill states "Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm." The data principal is only notified of the data breach if the Data Protection Authority of India determines that such breach should be reported to the data principal. This substantially takes away the data principal's right to be informed about breach of their personal data and leaves it at the discretion of the Authority.

I. Data Localization - Data localization laws intend to keep citizens' personal data in-country and subject to local regulations. Data localization is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated. Free flow of digital data, especially data which could impact government operations or operations in a region, is restricted by some

[11] *Id.*, s.23
[12] *Id.*, s.27(1)
[13] *Id*, s.27(1)
[14] *Id.*, s.27(2)
[15] *Id.*, s.27(3)
[16] *Id.*, s.27(4)
[17] *Id.*, s.27(5)
[18] *Id.*, s.32(1)

governments.[19]Section 40 of the Bill casts an obligation on the data fiduciary to store at least one serving copy of personal data on a server or data centre located in India.Clause 2 of the Section provides for categories of critical personal data, to be notified by the government that can only be processed in a server or data centre located in India. Further, Section 41 imposes conditions for cross-border transfer of personal data which include standard contractual clauses, necessity, and consent of data principal and intra-group schemes, inter alia. Internet by its architecture is open, unrestricted, and global and restricting the free-flow of the internet would violate the basic principles of 'World Wide Web'. Data localization requirements also interfere with the most important trends in computing today. They limit access to the disruptive technologies of the future, such as cloud computing, the "Internet of Things," and data-driven innovations (especially those relying on "big data"). Data localization sacrifices the innovations made possible by building on top of global Internet platforms based on cloud computing. This is particularly important for entrepreneurs operating in emerging economies that might lack the infrastructure already developed elsewhere. And it places great impediments to the development of both the Internet of Things and big data analytics, requiring costly separation of data by political boundaries and often denying the possibility of aggregating data across borders. Data localization or mirroring is untenable in present technological reality[20]. Localized data creates a "keeping all eggs in one basket" situation and makes user data more open to hacks. Studies have shown that in India, loss per worker would be nearly 11% of the average monthly salary if data retention requirements are imposed. Besides, a considerable loss in the domestic investment of 1.4% to 1.9% is also expected in India[21]. A study on economic losses caused by data localization shows a negative effect on GDP in all cases e.g. China (-1.1%), Vietnam (-1.7%)[22]. It adds that losses in India would be 0.1% of GDP for sectoral implementation of localization e.g. financial data under Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. But a blanket localization may raise the economic losses by eight times[23]. Data centres are highly energy intensive. Specialized cooling systems are required in data centres to keep their temperatures at an optimal level. Reports suggest, data centres are presently responsible for 2% of greenhouse gas emissions[24], which is at the same level as the aviation sector. These costs would be even higher in tropical countries like India where mean temperatures are comparatively high. Besides, proper electrical infrastructure needs to be ensured. Data localization may be disadvantageous to the IT sector and will prevent the free flow of data. Data protection is nonetheless important but hypersensitive and aggressive approach may do much harm than it may do any good. Options to enter into bilateral data sharing agreements, real-time data sharing etc. should be explored. Research reveals that no country has been too rigid vis-à-vis data protection and has adopted a balanced approach to balance privacy and data protection concerns on one hand and free internet on the other. Strategic and sensitive data, however, may be stored locally, but, making an umbrella provision applicable to all sorts of data without distinction may frustrate the very purpose of the Bill.[25]

J. Authorities under the Bill

The Data Protection Officer-The Bill envisages Data Protection Officer (hereinafter 'DPO') to be appointed by the data fiduciary. Under section 36, the manifold responsibilities of DPO include, advising data fiduciary on fulfilling data protection obligations, developing internal mechanisms based on "Privacy by Design", receiving grievances from data principal and raising them before data fiduciary etc. It assigns the DPO to monitor "personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act". Thus, independence of DPO is crucial considering his/her "whistle-blowing" role and the fact that he/she would still be an employee under the data fiduciary. However, no such protection has been afforded in the Bill.

The Data Protection Authority Of India- The report contemplated an independent data protection authority which materialized as the Data Protection Authority of India in the Bill. In principle the authority is independent, however, there are certain provisions in the Bill showing otherwise. The selection committee, to

[19] What is Data Localization?, *available at:* https://www.techopedia.com/definition/32506/data-localization (Last visited on March 6, 2019)
[20]Chander, Anupam and Le, Uyen P., Data Nationalism (March 13, 2015). Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947
[21]*Supra* note 44
[22] When the Cloud Goes Local: The Global Problem with Data Localization, *available at:* https://www.computer.org/csdl/magazine/co/2013/12/mco2013120054/13rRUxC0Srf (Last Visited on March 6, 2019)
[23] Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Verschelde, The Costs of Data Localisation: A Friendly Fire on Economic Recovery, *available at:* https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf *(Last visited on March 6, 2019)*
[24] The Guardian: How viral cat videos are warming the planet, *available at:* https://www.theguardian.com/environment/2015/sep/25/server-data-centre-emissions-air-travel-web-google-facebook-greenhouse-gas *(Last visited on March 6, 2019)*
[25]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at:* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3 (Last visited on March 6, 2019)

make selections to DPAI, is biased in favour of the Executive. On the surface it would appear that Section 50(2) of the Bill allows for the selection of the Chairperson and other Members of the Authority by a Committee consisting of the Chief Justice of India (CJI) or his/her nominee, the Cabinet Secretary and one expert of repute to be nominated by the CJI or his/her nominee in consultation with the Cabinet Secretary. However, as per Section 50(6), "The Central Government shall maintain a list of at least five experts". This means that the Executive has the power to curate the list of experts. The power of CJI or his/her nominee to nominate an expert in consultation with the Cabinet Secretary is limited to only those experts that have already been shortlisted by the Executive. Therefore, the Executive holds two out of three positions in the selection committee.[26]The possibility of executive influence brings the credibility of the Data Protection Authority under suspicion and sans an independent authority, the purpose of the Bill will get frustrated.

Adjudicating Officer- The Bill under Section 68(1) creates a separate adjudicatory wing of the Authority and to "to ensure the operational segregation, independence, and neutrality of the adjudication wing", the central government has been conferred with the power to prescribe – "(a) number of Adjudicating Officers; (b) qualification of Adjudicating Officers; (c) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers; (d) jurisdiction of Adjudicating Officers; (e) procedure for carrying out an adjudication under this Act; and (f) other such requirements as the Central Government may deem fit."[27] From the language of the section, it appears that the adjudicatory wing, while in principle a part of the authority, is expected to function independently. However, giving such comprehensive powers to the central government under Section 68(2) reveals juxtaposition. Considering the importance of the Adjudicatory Officer, clear criteria for their appointment should have been devised in the Bill itself as a replacement for leaving it to the whims and fancies of the government.

Appellate Tribunal- The Bill is, in reality, an extension of the Information Technology Act, 2000. The IT Act, 2000 allows for appeals against the order of a Controller of Certifying Authorities or an Adjudicating Officer to be filed at the Cyber Appellate Tribunal. Sadly though, the tribunal without a Chairperson has been dysfunctional ever since 2011. The fact that the IT Act prescribes no time limit for appointment of a Chairperson has left matters listed before the tribunal unresolved. Also, the formation of benches, distribution of business and transfer of cases between different benches can all be done only by the Chairperson. The absence of a Chairperson at any point in time would prove crippling to the Appellate Tribunal that would be established under this Bill, as already seen in the case of the Cyber Appellate Tribunal. The Bill has failed to address this issue and provide for a clause for timely appointment of a Chairperson of the Appellate Tribunal to adjudicate on appeals from the Data Protection Authority and adjudicating officers.Furthermore, disproportionate discretionary power has been given to the government vis-à-vis qualifications, appointment, term, and conditions of service of members[28] of the tribunal vide section 80. Appeals from the tribunal lie to the apex court[29] directly without any role of the jurisdictional High Court. This is contrary to the decision of the Hon'ble Supreme Court of India in the case of *L. Chandra Kumar v. Union of India*[30] wherein it was held that: "... the power vested in the High Courts to exercise judicial superintendence over the decisions of all Courts and Tribunals within their respective jurisdictions is also part of the basic structure of the Constitution."

K. Section 98 - The section empowers the Central Government to issue directions to the Data Protection Authority of India in certain cases. Though an opportunity of being heard is secured for the Authority, nonetheless, the directions of the Central Government are still binding on the Authority. This section is therefore startling as it gives extensive discretionary powers to the Central Government and has the potential to be misused by the executive. This calls the independence of the Authority into question. Contrasting are the provisions in EU wherein Data Protection Authorities are required to be independent.[31] The European Court of Justice has held in *Commission v. Hungary*[32] that establishment of an independent supervisory authority is an essential component of the protection of individuals with regard to the processing of personal data. Operational independence of supervisory authorities, in that members are not bound by instructions of any kind in the performance of their duties, is an essential condition that must be met to respect the independence requirement, but this is not sufficient. *The mere risk that the state could exercise political influence over decisions of a supervisory authority is enough to hinder independence.*

[26]*Supra* note 7
[27]*Supra* note 1, s.68(2)
[28]*Id.*, s.80
[29]*Id.*, s.87
[30] A.I.R 1997 SC 1125
[31]Treaty on the Functioning of the EU (TFEU), art.16 (2); EU Charter of Fundamental Rights, art. 8(3)
[32](C-288/2012)

L. Surveillance Reforms - The existing surveillance framework is complex and confusing. Simply put, two statutes control the field: telephone surveillance is sanctioned under the 1885 Telegraph Act (and its rules), while electronic surveillance is authorized under the 2000 Information Technology Act (and its rules). The procedural structure in both cases is broadly similar, and flows from a 1997 Supreme Court judgment: surveillance requests have to be signed off by an official who is at least at the level of a Joint Secretary.[33]Recently on December 20, 2018, the Ministry of Home Affairs issued an order authorizing 10 Central agencies to intercept, monitor, and decrypt "any information generated, transmitted, received or stored in any computer." Which raises serious concern for surveillance reforms.[34] "The Supreme Court in the *Puttaswamy* judgment admitted that the formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State. National security, data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries, and prevention and investigation of crime were considered to be legitimate aims of the State by the nine-judge bench. While the Committee has incorporated the tests laid down in the *Puttaswamy* judgment in Sections 42 and 43 of the Bill, there is no surveillance reform in the Bill. Even though the Report submitted by the committee acknowledges that it is critical to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception, the same has not been defined in the Bill. Any privacy law is inadequate without surveillance reform. The Report accepts that the design of the current legal framework in India is responsible for according a wide remit to intelligence and law enforcement agencies and lacks sufficient legal and procedural safeguards to protect individual civil liberties. It acknowledges that there is little oversight that is outside the executive to prevent the rise of a surveillance society. The report highlights the oversight mechanisms for surveillance used in other democratic countries and mentions that "*it is worthwhile to recognize that all the aforementioned jurisdictions provide some form of inter-branch oversight through a statute. Nothing similar exists in India. This is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional."* However, the draft bill suggests no amendment to laws that allow for surveillance. To ensure accountability and transparency and to balance the state's interests with the right to privacy of the data principal, we recommend that notice should be provided to the data principal after completion of the surveillance. The data principal must also have the right to challenge and seek redress against a surveillance order. Special tribunals for the purpose of reviewing all surveillance or interception orders issued by a competent authority under the Bill can be set up. The time period for which an interception or surveillance order is valid should also be prescribed in law."[35] In terms of our other suggestions, the draft law includes an obligation of fair and reasonable processing and ensuring the security of data even when such processing takes place under the given exemptions. It, however, fails to recognize other important requirements like having data protection officers inside intelligence agencies and LEAs; (deferred) notice to the concerned individual, and the right to seek appropriate redress. Further, the draft law also fails to address the issue of the evidentiary value of information collected in breach of the proposed data protection law. The draft law proposed by the Srikrishna Committee has tremendous scope for improvement, both in terms of strengthening the protections available to individuals who are subjected to surveillance activities as well as the structural and procedural safeguards governing such access. The recommendations contained in the report, particularly on ex-ante and ex-post safeguards against surveillance, are a significant starting point for this discussion. To take these suggestions to their logical conclusion, it is important that corresponding amendments should be made to the draft before it shapes into a bill that can be placed before the Parliament.[36]

III. CONCLUSION

If and when the Bill becomes an Act, India will join the list of countries that proactively protect the right to privacy of their citizens and in so doing, their personal data. Being the largest democracy of the world, India is being looked upon, especially in the time when the world has awaken in favour of high data protection standards, to set up the highest canons of privacy. This article has analyzed, compared and critically appraised the provisions of the Personal Data Protection Bill. The Bill, provides for data-principal rights; data-fiduciary

[33] The case against surveillance, *available at:* https://www.thehindu.com/opinion/lead/the-case-against-surveillance/article25822069.ece (Last visited on March 6, 2019)

[34] Centre's 'snooping' order kicks off political slugfest: All you need to know, *available at:* https://indianexpress.com/article/india/opposition-slams-govt-defends-surveillance-order-all-you-need-to-know-5504466/ (Last visited on March 6, 2019)

[35] *Supra* note 7

[36] Placing surveillance reforms in the data protection debate, *available at:* https://blog.theleapjournal.org/2018/08/placing-surveillance-reforms-in-data.html (Last visited on March 6, 2019)

obligations; child data protection; cross border transfer of data; Data Protection Authority and adjudicatory wing to redress grievances; an appellate tribunal, penal provisions; and more. At the same time, as the article shows, the Bill also misses on several aspects which were critically dealt with, followed by quite a few suggestions.

ACKNOWLEDGEMENTS

Deepest gratitude to Prof. (Dr.) Rajesh Bahuguna, Dean (Law), Uttaranchal University and Prof. (Dr.) PoonamRawat, HOD (Law), Uttaranchal University for their invaluable guidance.

IOSR Journal Of Humanities And Social Science (IOSR-JHSS) is UGC approved Journal with Sl. No. 5070, Journal no. 49323.

Karam Pratap Singh. "Critically Appraising the Personal Data Protection Bill, 2018." IOSR Journal of Humanities and Social Science (IOSR-JHSS). vol. 24 no. 04, 2019, pp. 57-63.