REMEMBERING TO FORGET: A LEGISLATIVE COMMENT ON THE RIGHT TO BE FORGOTTEN IN THE DATA (PRIVACY AND PROTECTION) BILL, 2017

*Navya Alam and Pujita Makani**

Abstract

The Supreme Court of India granted citizens with the fundamental right to privacy in 2017. The Court recognized the importance of individual autonomy and ability of an individual to exercise control over his personal information. The right to be forgotten is instrumental in enabling an individual to exercise such control.

The Data (Privacy and Protection) Bill, 2017 introduced in the Lok Sabha by Baijayant 'Jay' Panda, seeks to provide a statutory framework for data privacy, security and protection. Among other rights and duties, it includes the 'right to be forgotten' to ensure that individuals are protected from the misuse of personal data by data controllers and third parties. This paper highlights the salient features of the Bill. Through a close analysis of the Bill, particularly its language and the safeguards it proposes, the right to be forgotten seems to be diluted and potentially ineffective. We argue that the Bill has not

been contextualised in light of recent international developments. Further, the Bill must adopt consistent language to secure clarity in its interpretation. The Bill also needs to be industry and sector specific given the nature, size, infrastructure and operational capabilities of various industries.

I. INTRODUCTION

On 24th August 2017, a nine-judge bench of the Supreme Court unanimously affirmed that the right to privacy is a fundamental right under the Indian Constitution. The judgment recognizes that privacy includes "the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone."[1] It recognizes that privacy safeguards individual autonomy and enables an individual to control vital aspects of his or her life. By necessary implication, the right to be forgotten gives an individual the ability to exercise such control. The right to privacy judgment ushered in a new era in Indian constitutional law. It had an indelible impact on several issues, ranging from surveillance, data collection and protection to free speech and LGBT rights. The judgment also bolstered several legislative and policy questions. However, the judgement only marks the beginning. Of the many questions that must now be answered, the question of data security, privacy and protection takes precedence in light of the recent Aadhar controversy.

*Navya Alam and Pujita Makani are fifth-year students at the Jindal Global Law School. The authors may be reached at 13jgls-nalam@jgu.edu.in and 13jgls-pmakani@jgu.edu.in respectively.

[1]K.S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 641.

The Indian Parliament must now navigate a thicket of structural and technical questions before effectively introducing a data security framework in India. The Parliament must carefully deliberate upon the very conceptualisation of a data security framework in India. What might an Indian data protection law look like? How does the Parliament envisage the relationship between the right to privacy and data security? Further, how can private players aid the government in protecting the citizens' fundamental right to privacy? What is the nature and extent of the duty of private players in granting data security, privacy and protection? Additionally, the Parliament must consider technical questions such as the right to be forgotten and legislative and procedural safeguards in securing the individual's personal data.

Fortunately, the Data (Privacy and Protection) Bill, 2017, introduced by Baijayant 'Jay' Panda, a Member of Parliament from the Kendrapara constituency, provides a valuable starting point in answering such questions. The Bill seeks to legislate a comprehensive data privacy and protection framework that contemplates key policy questions crucial to securing the fundamental right to privacy for the citizens of India. The Bill raises several issues about data security law. However, this paper will only comment upon the right to be forgotten provisions in the Bill.

Section 10 of the Bill envisages the right to be forgotten. The right to be forgotten enables an individual to "determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."[2] The right to be forgotten is an important right, especially in the digital age, where personal data about individuals is readily available in the public domain. Such

[2]Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten,"* 29 COMPUTER L. & SEC. REV. 229, 231 (2013).

information might be outdated, embarrassing or irrelevant. In the absence of such a right, the availability of such information, when made without the individual's permission, is an infringement of the fundamental right to privacy. This poses a threat to one's virtual and physical reputation and security. However, in the absence of adequate safeguards, the right to be forgotten may run contrary to the essence of freedom of speech and expression.

Several European ideas have historically captured the essence of the right to be forgotten. For instance, under the Rehabilitation of Offenders Act in the United Kingdom, one's criminal convictions become immaterial while seeking employment opportunities or during civil proceedings after a given period of time.[3] The present-day understanding of the right to be forgotten has taken shape in the 2014 Costeja case.[4] Here, the European Court of Justice analysed the countervailing right to privacy and data protection with the right to information. Here, the Court placed precedence on an individual's right to privacy over the interest of the search engine and of the public. The Court held that Google violated a Spanish man's right to be forgotten by refusing to remove links that were irrelevant in light of the time that had elapsed. It further held that an "internet search engine operator is responsible for the processing it carries out of personal data, which appear on web pages published by third parties."[5] The Court's reasoning has been crystallized in right to be forgotten provision (Article 17) of the General Data Protection Regulation (GDPR), set to become enforceable from May 2018.

[3]Charles Arthur, *Explaining the 'right to be forgotten' - the newest cultural shibboleth,* THE GUARDIAN, (May 14, 2014), https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth.

[4]Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

[5]*Id.*

India is at crossroads. The right to privacy judgment is a positive step to secure data protection and privacy. However, the efficacy of the judgment is dependent on enacting several corollary rights, such as the right to be forgotten. An effective right to be forgotten will strike a balance between countervailing rights such as the individual's right to privacy and data security and freedom of speech and right to information.

Part I sets out the salient features of the Bill. Part II presents a critical analysis of the right to be forgotten provisions in the Bill.

II. THE DATA (PRIVACY AND PROTECTION) BILL, 2017

The Data (Privacy and Protection) Bill, (the "Bill") seeks to secure and protect data of individuals, and balance countervailing interests such as national security and the right to freedom of speech and expression. Further, the Bill emphasizes the need for and importance of privacy and data protection in light of increase in cyber-attacks and terrorist activities. It also has an overriding effect on the Telecom Regulatory Authority of India (TRAI), Information Technology (IT) and other Acts that pertain to the collection, processing, interception and monitoring of personal data.

The Bill lays a strong foundation for a robust data privacy protection law. Most definitions are precise; the full extent of terms like 'personal data' and 'sensitive personal data' has been clearly defined. This is a welcome change, since the Information Technology Act, 2000 makes no distinction between 'personal data' and 'sensitive personal data'. Further, the Bill is unequivocal in making a distinction between terms that are often used interchangeably, such as 'data controller' and 'data processor'. The clarity in definitions increases efficiency in enforcement.

The Bill stipulates the nature of consent, i.e. every individual *must* provide express consent for the collecting, processing, storing and disclosing of any personal data.[6] The consent is revocable at any time in the future. The Bill also grants an individual a qualified right to review, modify or remove their personal data. The request to remove personal data is allowed when (a) it fulfills the purpose that it was originally collected for, (b) it was unlawfully obtained, or, (c) the person revokes his consent.[7] This is particularly empowering in an age where several powerful data controllers make an unauthorized sale of an individual's personal data to third parties. Earlier, an individual would have no control if such information was sold or transferred to third parties situated both in India and in other jurisdictions. The Bill redresses this problem. Cross-border transfers - of information pertaining to an individual - to third parties are only allowed with the express consent of the individual.[8] Further, all third parties are expected to have similar data privacy and security provisions as the transferring party.[9] In the absence of similar data privacy and security provisions, third parties will not be allowed to receive data from the transferring party. Therefore, the Bill takes a holistic approach in ensuring data security and protection standards by extending the same to third parties.

Another positive step towards safeguarding data is the principle of minimisation, which stipulates that a data controller must only seek to collect and process information that is absolutely necessary. The Bill strikes a reasonable balance between the right of an individual and that of a data controller, more specifically, between those rights that arise or extinguish respectively when the purpose of collection and processing of personal data has been fulfilled, or ceases to exist.

[6]The Data (Privacy and Protection) Bill, 2017, Bill No. 161 of 2017, §.5(2).
[7]*Id.* §10.
[8]*Id.* §25
[9]*Id.* §24.

Section 23(3) of the Bill allows for the prolonged storage of personal data in specific situations such as statistical or research purposes. However, the proviso creates a margin of necessity by distinguishing between necessary and unnecessary personal data. Parts of the data that is are not required for the purposes specified in Section 23 are separated from the whole and is destroyed. This provision is a clear illustration of the principle of data minimisation, which ensures that the right of removal of personal data is not completely diluted even when the legislature provides certain leeway to the data controller.

The Bill also provides for the constitution of a Data Privacy Authority. The function of the Authority is to ensure compliance with the provisions of the Bill. The Authority undertakes inspection and impact assessment to ensure compliance with the Bill. It also has the power to adjudicate on matters arising from the Bill and impose punishments. Therefore, these procedures give teeth to the legislation.

III. CRITICAL ANALYSIS OF THE RIGHT TO BE FORGOTTEN PROVISION IN THE BILL

The following section presents a critique to of the Bill on grounds that (1) the Bill has not been situated within the current global data security protection climate, (2) the language of the Bill is unclear and creates ambiguity in understanding the provisions relating to the right to be forgotten and (3) the Bill does not contemplate adequate safeguards to ensure an effective implementation of the right to be forgotten.

C. Contextualization of the Bill

The Bill must be contextualised keeping in mind the current global data security protection climate.

For instance, the European Union has methodically created a robust framework of law that is "economically dominant, locally secure, and morally defensible."[10] The cornerstone of the EU data framework is protecting individuals' data while simultaneously bolstering the economy's growth. To achieve this, the EU and the European data industry have entered into a public-private partnership worth $2.5 million that "aims to strengthen the data sector and put Europe at the forefront of the global data race."[11] Further, the EU has decided to overrule the existing e-privacy directive. The existing directive was limited to traditional forms of communication. The EU now wants to include "Over-The-Top" services such as WhatsApp and Facebook[12] within its directive. This means that the user must grant explicit consent for internet companies to record and store communications for advertising purposes.

The Bill takes a blanket approach to data privacy and protection. Each industry and sector varies in its nature, size, operations, infrastructure and capabilities. As a result, every industry collects and processes personal data in varying capacities. Therefore, each industry and sector has different obligations towards data subjects. Thus, the Bill must be inclusive of such differences. Further, a blanket approach overlooks the sensitivity of data that is sector specific, and consequently, the timeline of its erasure. Therefore, the right to be forgotten provisions must be viewed through the lens of such sectoral challenges, and not despite it.

[10]Kathryn Witchger, *The Great Data Race: Lessons from EU Cyber Law*, COLUMBIA JOURNAL OF TRANSNATIONAL LAW (Oct. 14, 2017, 2.40 PM), http://jtl.columbia.edu/the-great-data-race-lessons-from-eu-cyber-law/.

[11]European Commission, *European Commission and data industry launch €2.5 billion partnership to master big data*, (Oct. 13, 2014), http://europa.eu/rapid/press-release_IP-14-1129_en.htm.

[12]Samuel Gibbs, *WhatsApp, Facebook and Google face tough new privacy rules under EC proposal*, THE GUARDIAN, (Jan. 10, 2017), https://www.theguardian.com/technology/2017/jan/10/whatsapp-facebook-google-privacy-rules-ec-european-directive.

D. Language and Structure of the Bill

Only four instances trigger the application of Section 10 (the right to be forgotten). First, when the purpose for collecting or processing of the data is satisfied, second, when consent is withdrawn, third, when personal data is collected unlawfully, and lastly when erasure is mandated by a court order. The act of unlawfully processing personal data however does not trigger the application of Section 10 directly. The Bill lays out a comprehensive and extensive definition of 'processing'. Processing of data includes obtaining but also recording, organization, adaptation, alteration, retrieval, dissemination, etc.[13] It is of concern that 'unlawful processing' of personal data has been overlooked as a ground for seeking removal of personal data. This is possible only through a court order. Therefore, this creates a significant barrier to invoke the right to be forgotten when the unlawful processing of data ought to be regarded in the same light as unlawful collection of such data. This means that, the Bill might not be able to offer immediate protection for individuals who want to remove personal data where a data controller has adapted such personal data and disseminated it. In practice, the failure to include 'unlawful processing' as a ground will render the right to removal of personal data nugatory.

Second, Section 10 fails to address situations where time is of the essence. The expeditious removal of personal data is crucial for an effective implementation of the right to be forgotten. Technology allows for an exponential reach and instantaneous dissemination of information. Therefore, any potential misuse of personal information would be difficult to reverse if there is any delay on part of the data controller. Keeping in mind the available technology and the cost of implementation it would be beneficial if the data controller is obliged to take steps to prevent undue delay in determining the request of removal. The Bill does not stipulate a reasonable period or parameters to determine an undue delay or discourage the same.

[13]The Data (Privacy and Protection) Bill, 2017, Bill No. 161 of 2017, §2(n).

Third, the Bill fails to balance the rights and duties that it confers upon the individual and to data controllers. Section 10(1) provides for the 'removal' of personal data of individuals if the personal data is no longer necessary after the original purpose of collecting and processing has been satisfied. However, Section 23 prohibits the unnecessary storage of personal data by persons, and such persons must 'destroy' such data if the purpose of collection is achieved or ceases to exist.[14]

If the intended purpose of the statute is to discourage unnecessary collection of data, then the inconsistent language used in these sections does little to demonstrate it. The implications of 'remove' and 'destroy' suggest different and unequal approaches to the same problem. In common parlance, 'remove' and 'destroy' could possibly achieve the same result i.e. the non-existence of the personal data. However, given the use of the different terms within the Bill it would imply that 'removal' is an operation that is not as permanent as the 'destruction' of data, or that it might allow the possibility of recovery. Thus, this could be used as a potential loophole to circumvent the provisions of the Bill.

E. Lack of adequate safeguards

The Statement of Objects and Reasons draws to an end after declaring "the Bill seeks to codify and safeguard the right to privacy for all juristic persons in the digital age, balanced with the need for data protection in the interests of national security."[15] However, this is merely the beginning. The safeguards contemplated by the Bill are insufficient to effectively safeguard the right to privacy. As a consequence, it would impede the right to forget.

Section 26 of the Bill suggests that pseudo-anonymization will be

[14] *Id.* §23(2)

[15] *Id*. Statement of Objects and Reasons.

encouraged in matters related to collecting, processing, storing, disclosing and/or handling personal data.[16] Pseudo-anonymization refers to processing personal data in a manner that it is no longer attributable to a specific person without additional information. The Bill only encourages pseudo-anonymization, as opposed to mandating the same. Pseudo-anonymization is a feeble promise in the absence of a larger framework that clearly defines its working. The Bill must include, or provide for the inclusion of, general principles of data protection for all organizations that collect and process an individual's personal data. The principles must stipulate a clear timeline for the pseudo-anonymization of data. Further, the Bill must make 'privacy by design' a legal requirement. 'Privacy by design' ensures that every new organization that collects or processes personal data is obliged to take the protection of such data into account.[17] Making 'privacy by design' a legal requirement will ensure that data security is complied with from the outset.

To ensure compliance with the request made under Section 10, data controllers should maintain a record of removed data. It should include which data was removed, what method was used to remove such data, the extent of removal, and by whom the data was removed by to ensure accountability. Such records must not disclose any information that might lead to the identity of the individual being disclosed. This could possibly ensure compliance with the provision and make the right to be forgotten a reality rather than a hollow promise.

Additionally, given the rapid growth in technology, especially concerning storage, the method of removal should be able to keep pace with such advances. The methods of removal of different records should be regulated through guidelines, or an established and standard procedure must be implemented, to ensure that the data is not

[16] *Id.* §26.

[17] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECHNOLOGY L. J., No. 2 1333, 1413 (2013).

recoverable.

The Bill fails to realise the extent to which personal data can be processed, once shared by the data controller. Mere removal of such data by the data controller does not tie all loose ends. In order for Section 10 to be robust, it is pertinent to make it mandatory for data controllers to inform other data controllers who are processing such personal data to erase any links or copies of the concerned data, following the request.

IV. CONCLUSION

The Bill is a positive step towards securing data privacy and protection in India. However, it is riddled with loopholes that curtail the right to be forgotten. The Bill has to employ uniform terminology, particularly to define terms such as 'removal', 'destroy' and 'erasure'. The terms have been used in different contexts and the distinction between them is unclear. The Bill must lay down an expeditious procedure to respond to requests for the removal of personal data. Further, the Bill must streamline the manner in which data is removed, so as to ensure that there is no unauthorized dissemination following advancement in technology. Finally, data is often transnational in nature, and therefore must be compatible with the global data security climate.