PROTECTION OF RIGHT TO BE FORGOTTEN ON SOCIAL MEDIA IN THE CONTEXT OF DATA PROTECTION BILL 2019 OF INDIA

—Anand N Raut[*] & Arpita Verma[**]

Abstract—More than have of the World is on social media. Almost every user post information which is sensitive or personal in nature. Protection of such data falls within the ambit of right of privacy. Personal Data Protection Bill 2019 which protects various facets of personal data and its usage, flow etc. also bestows right to be forgotten. Users of social media also enjoy freedom of speech and expression and right to information etc. There is viable possibility of collision amongst these rights. The paper aims study whether draft bill to solve the possible collision that emerges between the right to be forgotten and other fundamental rights like the access to knowledge or the freedom to speech in the setting of social media. The discussion in paper is based on five-point criteria for balancing the conflicting rights provided in the Personal Data Protection Bill 2019.

Keywords: Right to be Forgotten, Social-Media, Personal Data Protection Bill.

[*] PhD & Assistant Professor (Law), Maharashtra National Law University, Mumbai (Maharashtra). <anand@mnlumumbai.edu.in>.

[**] PhD candidate, Faculty of Law, The University of Tasmania, Australia.

I. INTRODUCTION

The *Right to be forgotten* a facet of Right to privacy is one of the most discussed, controversial but vital data protection legal right of the decade and is likely to remain so in the following years.[1] It originated in European legal context[2] as a way of "strengthening individuals' control"over their own identity and data *over internet*[3] *by vesting them with power to remove their personal data from i*nternet search engines or websites.[4]

In India, the debate upon right to be forgotten emerged after 2017 Supreme Court decision of *K.S Puttaswamy* v. *Union of India*[5] where for the first time right to privacy was defined to include right to be forgotten. Subsequently, Justice B.N. Shrikrishna Committee (Data protection committee)[6] made a recommendation to include right to be forgotten as a statutory right under the Personal Data Protection Bill, 2019.[7]

In the specific context of social media,right to be forgotten gains a specific importance considering the amount and diversity of personal data shared on social media[8] and the permanent nature of the data itself.[9] The data shows, social media companies are one of the key subjects of de-listing requests made by individuals in 2020.[10] Intermediary rules[11] does impose duty on intermediaries of removing or disabling access to certain problematic type of content[12] which is hosted, stored, published or transmitted by it. The Rules also obliges significant social media intermediary to use technologies and notify users attempting to access removed content.[13] Such measures being inadequate and considering the significance of the right to be forgotten, it necessitates a careful overview of the said right as defined by the draft bill and its impact on social media. Precisely this is the aim of the article.

The article consists of three parts. Part 1 provides the descriptive view of the right to be forgotten as adopted by Indian Personal data protection bill, 2019 (draft bill). Part 2 provides an analysis of how the draft bill aims to achieve balance between right to be forgotten of one person against constitutional rights including right to information or right of freedom of speech and expression of others via the five criteria provided in the bill. Part 3 contains a summary of conclusion, key findings, recommendations and way forward.

---

1 Minhui Xue et al., "The Right to be Forgotten in the Media: A Data-Driven Study," 4 Proc. Priv. Enh. Technol. 389, 390 (2016).

2 Jeffrey Rosen, "The Right to be Forgotten," 64 Stan. L. Rev. Online 88, 88 (2012).

3 Meg Leta Ambrose & Jef Ausloos, "The Right to be Forgotten Across the Pond," 3 J. Inf. Policy 1, 11 (2013).

4 Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (*Google Spain case*), ECLI:EU:C:2014:317 (May 13, 2014).

13 Rule (4)(4) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

II. RIGHT TO BE FORGOTTEN IN INDIAN DRAFT PERSONAL DATA PROTECTION BILL 2019

Section 20 of the draft bill sets forth the provision for right to be forgotten (RtbF) or as the section terms it: "right to restrict or prevent continuing disclosure of personal data." Individuals can exercise this right in the following three scenarios:

"a) The consent necessary to collect and process data has been withdrawn, or;

b) Data is being used in a manner that is contrary to the provisions of the law, or;

c) Disclosure of data is no longer necessary."

The right is not absolute and legitimacy of the individual's claim has to be proved to an adjudicating officer established under the bill.[14] Consequently, before making any order enforcing the removal of data, adjudicating officer will have to carefully weigh in the data principle's right to prevent or restrict the continued disclosure of data against constitutional rights of other citizens'.[15] An additional clause in the section, establishes a five-point criteria that should be considered by the Adjudicating officer when determining whether RtbF may be adopted.[16] These are:

The sensitivity of the personal data;

a) The scale of disclosure;

b) The role of the data principal in public life

c) The relevance of the personal data to the public; and

d) The nature of the disclosure.

In the European Union (EU) Privacy Act: General Data Protection Regulation, 2018 (GDPR),[17] RTF is provided in besides the right to erasure, which is on the lines of decision given "Google Spain" case.[18] The difference between the two is that the right to erasure allows the users to "fully" and "permanently"[19] delete all personal data from public source and private

[14] The Personal Data Protection Bill, 2019, S. 62.

[15] *Id.* at S. 20 (2).

[16] *Id.* at S. 20 (3).

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 OJ L 119/1.

[18] Case C-131/12Google Spain SL and Google Inc. v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González (Google Spain Case), ECLI:EU:C:2014:317 (2014).

[19] Aurelia Tamò & Damian George, "Oblivion, Erasure and Forgetting in the Digital Age," 5 J. Intell. Prop. Info. Tech. & Elec. Com. L. 71, 72 (2014).

storage[20] whereas, the RtbF largely aims to restrict or prevent continuous disclosure by deletion from public space only (such as delinking of data from search engines) and not private storage.[21]

The draft bill generally entitles users only with the RtbF and the right to erasure is limited to cases where the erasure of personal data that is no longer necessary for the purpose for which it was processed.[22] In general, right to erasure is also available, on grounds of morality in cases including sexual violence,[23] non-consensus disclosure of person's body[24] or personal data[25] and personal grievances.[26]

III. ANALYSIS OF 'RIGHT TO BE FORGOTTEN' IN SOCIAL MEDIA UNDER DRAFT BILL

In order to study the impact of RtbF in social media, one must examine and analyze at the very minimum how balancing test provided in the draft bill can be applied in the social media context. Precisely this will be carried out next with respect to each of the five criteria specified in the balancing act namely: "(1) The sensitivity of the personal data sought to be restricted; (2) The scale of disclosure or degree of accessibility sought to be restricted; (3) The role of the data principal in public life;(4) The relevance of the personal data to the public; and (5) the nature of the disclosure".

A. The sensitivity of the personal data

The draft bill recognizes that not all personal data are same and some data, due to their nature, might require higher standard of protection. Thus, the draft bill, distinguishes between two types of data: a) Personal data and b) sensitive personal data.

a) Personal data: "Personal data" according to the draft bill means

---

[20] W. Gregory Voss & Céline Castets-Renard, "Proposal for an International Taxonomy on the Various Forms of the Right to be Forgotten: A Study on the Convergence of Norms," 14 Colo. Tech. LJ. 281, 340 (2015).

[21] *Karthick Theodre* v. *Madras High Court*, 2021 SCC OnLine Mad 2755 (Court refused to "literally strike of the name of the person from the order or judgment which recorded the acquittal of the person from the criminal proceedings"); *Zulfiqar Ahman Khan* v. *Quintillion Businessman Media (P) Ltd.*, 2019 SCC OnLine Del 8494 (court ordered the publisher to remove certain publications from public space but allowed them to keep copies of the article in their private space).

[22] The Personal Data Protection Bill 2019, S. 18(1)(*d*).

[23] *Subhranshu Rout* v. *State of Odisha*, 2020 SCC OnLine Ori 878.

[24] X v. https://www.youtube.com/Watch?V=Iq6k5z3zys0 and Ors. *CS(OS) 392/2021.*

[25] *Banners Placed on Road Side in the City of Lucknow, In re*, 2020 SCC OnLine All 244.

[26] (Name Redacted) v. Registrar General, *WP (Civil) Nos. 36554-36555/2017.*

> "data about or relating to a natural person who is directly or indirectly identifiable whether online or offline or by inference drawn from such data for the purpose of profiling."[27]

Since the 1980s,[28] this identifiability test has been used to determine whether or not a piece of data is personal. However, with the development in the field of data science, the understanding of identifiability has changed considerably and data can no longer be classified as just identifiable or non-identifiable.[29] This makes it necessary to adopt a definition of personal data that can keep up with the changes in the way individual's data is collected, handled and processed.

In this regard, the definition of personal data proffered by the draft bill has an advantage of being both sufficiently general and technologically neutral. Consequently, it can be successfully adopted in varied contexts including that of social media.

b) Sensitive personal data: Amplification of protection is needed for some data processing because the nature of the data makes it more dangerous to individuals.[30] For instance, criminals may exploit a person's credit and debit card numbers or aadhar number in identity theft or other crimes against them. "Sensitive personal data" refers to such information that needs extra security.

Before the draft bill, the Privacy Rules established under the IT Act[31] categorises certain kind of data as sensitive personal data. However, the SPD rule suffers from certain limitations. For instance, a number of categories of personal data are excluded from the restrictive definition of sensitive data. Contracts may override SPD regulations.[32] The rules also are not applicable to "registered societies, registered association,"[33] and the "law enforcement agencies."[34]

Recognising the inadequacies of SPD rules, data committee re-defined sensitive data to include a non-exhausting list of data such as official identifier,

---

27 The Personal Data Protection Bill, 2019, S. 3 (28).

28 Organisation for Economic Co-Operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 7 (2013), <http://www.oecd.org/digital/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>. (Accessed on 26 September 2021).

29 World Economic Forum, Unlocking the Value of Personal Data: From Collection to Usage 8 (2013), <https://www.weforum.org/reports/unlocking-value-personal-data-collection-usage/>. (Accessed on 23 September 2021).

30 Data Protection Committee Report, *supra* note 6 at 24.

31 The Information Technology Act, 2000, S. 43-A (2000).

32 The Information Technology Act, 2000, SPD Rules, R. 4 (2011).

33 The Information Technology Act, 2000, SPD Rules, R. 8 (3).

34 The Information Technology Act, 2000, R. 2(1)(*c*) SPD Rules.

transgender status etc.[35] The committee also established factors to be considered when identifying what is sensitive personal data.[36] This is different from GDPR[37] which allows data processor to determine for themselves the nature of personal data where, the data has not been previously identified as sensitive data under the regulation.

Thus, criteria laid down in the bill removes (at least some) undue burden placed on the data fiduciary, by prescribing a minimum set of standards that should be considered by them while categorising the personal data as sensitive data. The aforementioned criterion is established under Section 15 of the draft bill and includes:

a. "Type of harm caused to individual due to processing of their personal data. If the harm is "significant"; it's probable that piece of data in question is sensitive personal data.

b. Expectancy of confidentially attached to the personal data. For instance, the health reports are expected to be confidential and thus are considered sensitive personal data.

c. Whether disclosure of personal data causes harm of a similar or relatable nature to a "significantly discernible class of data principals."

d. The adequacy of protection ordinarily available to personal data."

The power to postulate further type of sensitive personal data under the draft bill has been vested with the data protection authority established under the act.[38] In addition to the personal data and sensitive data, the draft bill also specifically defines three separate categories of data: Health data,[39] financial data[40] and genetic data.[41] However, all three categories are considered as sub-categories of sensitive data and must be afforded protection accordingly.[42]

B. The scale of disclosure and the degree of accessibility sought to be restricted or prevented

This requirement acknowledges the need to strike a balance between the data subject's right to privacy and the third party's right to free speech. Article 19(1)(a) of the Constitution[43] guarantees right to free speech and expression to every individual. This right is not absolute and state can make laws to impose

35 The Personal Data Protection Bill 2019, S. 3 (35).
36 *Id., at* S. 15.
37 General Data protection Act at Arts 6 and 9.
38 The Personal Data Protection Bill, 2019, S. 62.
39 The Personal Data Protection Bill, 2019, S. 3 (21).
40 *Id.*, at S. 3(18).
41 *Id.*, at S. 3(19).
42 *Id.*, at Ss. 3(35)(*iii*)(*ii*)(*viii*).
43 The Constitution of India, 1950, Art. 19(1)(*a*).

"reasonable restriction"on the right. Various courts have deliberated in detail about what amounts to "reasonable restrictions".[44]

On the other hand, in India, the right to privacy was just recently given specific constitutional status as a basic right.[45] While normally, it would have been adequate to refer the past jurisprudence to determine how both these rights can be balanced, the draft bill changes the factors to the balance by enabling protection against privacy risks originating from not just state but also non-state actors.[46] As a result, social networking platforms are legally required to respect the data principal's privacy.

The implications of this can be studied by looking at three common instances in which RtbF can occur on social media, as described by Peter Fleischer[47]:

a) "When a person shares a photo of himself on a social networking site and then requests the RtbF by deleting the photo."

As previously noted, social media websites have to respect individual's privacy rights including their RtbF. Thus, almost all the major social networking sites have to allow individual to delete their posts. While theoretically,they do comply with the condition; in practice the situation might be different. If the deleted Tweet is removed from the aggrieved person's account, any accounts that follow them, and Twitter search results on twitter.com. Likewise, Facebook.[48] and Instagram[49] also provide the option to delete posts, videos and photos. However,if a third person cross-posts the tweet of the aggrieved individual's somewhere else, it cannot be deleted.[50]

b) When individuals' share personal data related to their friends and family, or other individuals in addition to their own personal data.

---

[44] See e.g, *A.K. Gopalan* v. *State of Madras*, AIR 1950 SC 27; *Maneka Gandhi* v. *Union of India*, (1978) 1 SCC 248: AIR 1978 SC 597, *Brij Bhushan* v. *State of Delhi*, AIR 1950 SC 129, *Navtej Singh Johar* v. *Union of India*, (2018) 10 SCC 1.

[45] *K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1: AIR 2017 SC 4161.

[46] The Personal Data Protection Bill, 2019, S. 2 (A)(*b*).

[47] Peter Fleischer, "Privacy?: Foggy Thinking About the Right to Oblivion," Peter Fleischer Blog (March 9, 2011), <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.

[48] Facebook, "How do I Delete a Photo or Video From My Story on Facebook?", <https://www.facebook.com/h elp/1660071974290052?helpref=search&sr=10&query=delete> (last visited September 21, 2021).

[49] Instagram, "Editing and Deleting Posts", <https://help.instagram.com/997924900322403/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Using%20Instagram&bc[2]=Sharing%20Photos%20and%20Videos> (Accessed on 21 September 2021).

[50] How to delete a tweet, <https://help.twitter.com/en/using-twitter/delete-tweets> (Accessed on 21 September 2021).

In such cases, reference is to be made to the principle of "domestic exemption" included under the draft bill.[51] The exemption establishes that certain processing activities that are carried out by an individual for a purely personal or domestic purpose must be excluded from the scope of data protection. The genesis of this principle can be found in Swedish case of Lindqvist,[52] where the plaintiff had published personal data of her colleague such as their foot injury without their permission in a publically available website. The court held that website was not maintained for "personal reasons" because the data was knowingly made available to "infinite amount of people." Thus, plaintiff was considered as "data processor" and held liable for violation of privacy.[53]

The assumption here is that individual who makes their personal data publically accessible via social media websites must have done so knowing that it will be exposed to unidentified and indefinite amount of strangers.[54] Therefore, for instance,if Sunil posts a picture, what is important here is to determine Sunil's privacy settings.[55] Personal data distributed on the internet can easily be accessed by anyone, if it is posted to a public forum such as Facebook, Twitter or Instagram and will not qualify as personal or domestic processing[56] However, if it was only shared with a limited number of "friends," then the domestic exemption would apply.[57]

Sometimes however, it's not just the question of whether data is publicly or privately available but, also the nature of the post itself. For instance, a person publishing recipe online for his own personal enjoyment is different from a restaurateur doing the same.[58] Therefore, Section- 36(d) of the draft bill clarifies that personal or domestic exemption will not involve personal data processed for any professional or commercial purpose.

Apart from above, it's not clear what other guidelines could be used to decide which private post falls under domestic exception. Thus, it is imperative to issue certain guidelines especially in the context of social media as publishing personal data by individuals on social media means data processing activity might simultaneously be eligible for protection under personal or domestic exemption and other exemptions, mainly juristic expression.[59] For instance, an

---

51 The Personal Data Protection Bill 2019, S. 36 (*d*).

52 Case C-101/01, *Bodil Lindqvist* v. *Åklagarkammaren i Jönköping*, EU:C:2003:596.

53 *Id*. at 47.

54 Adam D. Moore, Privacy Rights 28 (2010).

55 Fiona Brimblecombe and Gavin Phillipson, *Regaining Digital Privacy: The New Right to Be Forgotten and Online Expression*, 4 Can. J. Comp. & Contemp. L. 1, 29 (2018).

56 Norberto Nuno Gomes de Andrade, *Oblivion: The Right to be Different... from Oneself: Re-proposing the Right to be Forgotten*, *in The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* 65, 72 (Alessia Ghezzi et al., eds., 2014).

57 *Ibid*.

58 Mariusz Krzysztofek, GDPR: Personal Data Protection in the European Union § 3.04 (2021).

59 *Ibid*.

individual's personal blog might become of public interest if she accidently recorded a group of pickpockets committing theft and uploaded it to her blog.[60]

To solve these problems; the committee report[61] does stipulates that in any such Indian context specific guidelines will be evolved through case laws in due course. A pertinent question to examine in the mean while is whether EU style guidelines offered by EU's Data Protection Working Party[62] would work in India? These guidelines include:

a. Does the individual posting the personal data have a household or personal relationship with the person posting it?

b. Whether processing of personal data is professional or full-time activity?

c. Are posts made by a number of individuals acting together in a collective and organised manner?

d. Is there the potential adverse impact on individuals, including intrusion into their privacy?

In the authors opinion, the EU guidelines are sufficiently generaland should be considered by the adjudicating officer before making any order related to individual's RtbF.

c) If a person posts something, and someone else copies it and re-posts it on their site, does the aggrieved person have the right to delete it?

Here the person has two options:(a) judicial procedures; which are expensive and time-consuming or (b) approaching platform where the content was first posted,however, the content would only be removed if it violates Platform's terms of service.[63] Thus, the platform is left in a predicament of having to balance between aggrieved individual's privacy claim and secondary writer's freedom of expression. The situation becomes more problematic if person sharing the personal data (say photo) on social media platform shares the frame with another person.[64]

---

60 Brittany Vonow, Female Pickpocket Gang Caught on Camera Swiping Tourist's Purse at Crossing, *The Sun* (June 28, 2019), <https://www.thesun.co.uk/news/9394618/female-pickpocket-tourist-steal/>. (Accessed on 23 September 2021).

61 Data Protection Committee Report, *supra* note 6 at 142.

62 Art. 29 Data Protection Working Party, *Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package,* (2013) Annex. 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities 9, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en>. (Accessed on 23 September2021).

63 Peter Fleischer, *supra* note 44.

64 Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the Right to be Forgotten in Big Data Practice," 8 SCRIPTED 229, 238 (2011).

According to Facebook policies, aggrieved individual can't delete the posts other have made in their timeline regarding them. However,they can only ask to be untagged from their timeline in which case their followers and friends won't see the post but the post will still exist,[65] similarly aggrieved individual can hide the posts but these only removes the post from their timeline, and not Facebook.[66] If someone wants to remove content submitted by others, they can do so, but only if the content is undesirable (nudity, harassment, spam, terrorism etc). Even outside the EU, a privacy breach form can only be filled out in the case of identity theft or the release of sensitive personal information such as full address or photo of residence, or any content that supports privacy theft.[67]

The other social media platforms like, Instagram only allows option to un-tag from the posts.[68] Twitter allows originator of tweet to delete there tweets of their tweet. However, if someone copies and paste part or all of originator's text into their own tweet, the latter tweet will not be deleted. Also, if somebody re-tweets the tweet after adding a comment, the re-tweets will not be removed.[69] As a result, there is a need for a rule on how someone else's freedom of speech can be constrained by someone else's right to be forgotten.

C. The role of the data principal in public life

A person is called a "public figure" if they occupy a public position or play a role in public life, such as in the arts.,[70] "economy, social sphere, politics,"[71] "sports or in any other domain."[72] The data protection committee report clarifies that a public figure is "someone who is either publicly recognisable or he/she serves in public office."[73] The rationale behind it is that an expectation of privacy reduces with increase in public status.[74] Therefore, the fact that a com-

---

[65] Facebook, "What if I Don't Like a Photo I'm Tagged in on Facebook?", <https://www.facebook.com/help/212466865441659?helpref=search&sr=4&query=untag> (last visited September 23, 2021).

[66] Facebook, "How do I Remove Something Posted on my Facebook Timeline?", <https://www.facebook.com/help/261211860580476?helpref=search&sr=7&query=hide%20post> (Accessed on 23 September 2021).

[67] Facebook, "Privacy Violations and Image Privacy Rights," <https://www.facebook.com/community standards/ privacy_violations_image_rights> (Accessed on 23 September 2021).

[68] Instagram, Tagging and Mentions, <https://help.instagram.com/627963287377328/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Using%20Instagram&bc[2]=Sharing%20Photos%20and%20Videos> (Accessed on 23 September 2021).

[69] Twitter, "How to Delete a Tweet," <https://help.twitter.com/en/using-twitter/delete-tweets#> (last visited September 23, 2021).

[70] See e.g. *Bobby Art International* v. *Om Pal Singh Hoon*, (1996) 4 SCC 1.

[71] See e.g. *People's Union for Civil Liberties* v. *Union of India*, (1997) 1 SCC 301: AIR 1997 SC 568.

[72] See e.g. *JIH* v. *News Group Newspapers Ltd*., 2010 EWHC 2818; *Hosking* v. *Runting*, 2004 NZCA 34.

[73] Data Protection Committee Report, *supra* note 6 at 171.

[74] *Hosking* v. *Runting*, 2004 NZCA 34.

plainant is a public figure may be an important factor in assessing whether or not RtbF should be granted to him or her in a given case. Further, additional factor to consider is what the kind of public figure is the aggrieved individual.

According to the draft bill "any person who is publically recognizable" will be a public person. However, in many situations fame can bear no relationship to role a person plays in public. Let us consider the example of Muhammad Sarim Akhtar better known as "Disappointed fan."[75] He acquired the moniker when his reaction during Pakistan vs Australia cricket match was captured during a live telecast which then later became viral in India. According to draft bill's definition, since Sarim Akhtar has become a nationally recognised figure, he should be considered as a "public figure." As a result, he may become the focus of media attention and be denied privacy, which is manifestly unjust to him.

This is what the data committee report presents as a criterion when it assesses "the role of a person in public life." The definition appears ambiguous. Should an actor who raises awareness of social concerns through his films be considered to have a "public role"? Does this imply that the draught measure only applies to public officials, who clearly play public roles? Such vague criteria fail to recognise the distinction between legitimate and illegitimate public interest in the life of a public figure.

The following may be incorporated in the draft bill to address such problems to a great extent.

> **a) Can voluntary discourse of personal data by public figure be considered as waiver of their privacy right?:** Lack of privacy is a part of being a star, athlete, artist, or politician, but is every aspect of their existence subject to invasion of private? Presumably not; alternatively, the personal data that the public figure "voluntarily released" or should have expected to be disclosed to the public can be waived.[76] While the voluntariness of disclosure can be easily proven, the foreseeability of information disclosure is not. An important test that can help answer the question here is "reasonable expectation of privacy" test established under the British jurisprudence.[77] Granted, it's expected that this test would necessarily need to be modified for Indian context.

---

[75] Akanksha Saxena, "'Disappointed Pakistani fan' aka Sarim Akhtar Features in Hong Kong Memes Museum" (2021), *Times Now* (August 1, 2021), <https://www.timesnownews.com/the-buzz/article/disappointed-pakistani-fan-aka-sarim-akhtar-features-in-hong-kong-memes-museum/793259>.

[76] *K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1: AIR 2017 SC 4161.

[77] See e.g. *Murray* v. *Express Newspapers Plc*., 2007 EWHC 1908; *Campbell* v. *MGN Ltd*., (2004) 2 AC 457: (2004) 2 WLR 1232.

b) Spectrum of publicity

Rather than treating all the public personality as same the draft bill or the rules should provide different rule for different category of individual. Here, the categorisation of individual is done on the bais of where they lie in the "spectrum of publicity" established by EU Advisory Council report.[78] The three categories include:

i. Individuals with clear roles in public life

This would include sportsman, artists, criminals, religious leaders, politicians, celebrities and CEOs. A person in this category is less likely to get delisting request approved as it's highly probable that information concerning them is public's overriding interest. For instance, H. Y. Meti, was the former Excise Minister of India. A video surfaced online that allegedly showed him and a woman in a compromising position.[79] If Meti were to make a delinking request, it might be rejected because public has legitimate interest in knowing his alleged crimes.

ii. Individuals with a limited or context-specific role in public life

It includes individual like public employees or those who accidently enter the public eye such as the singer Ranu Mondal (who became famous when a video of her singing in railway station became viral).[80] Graux[81] describes them as a person who had "temporarily entered the public limelight" and so far, been unsuccessful in "getting rid of unwanted attention" heaped upon them. Request of delisting made by these individuals will likely "weigh more heavily" than individual with clear role in public life.

iii. Individuals with no discernible role in public life

Certain organisations, such as media firms, have long had the ability to disseminate personal information about others. However, with the introduction of

---

[78] Article 29 Working Party, Opinion 5/2009on Online Social Networking (2009) , <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en>. (Accessed on 25 September 2021).

[79] Vikram Gopal, "Karnataka Excise Minister HY Meti Quits Over Sex Scandal Allegations," *Hindustan Times* (December 14, 2016), <https://www.hindustantimes.com/india-news/karnataka-excise-minister-h-y-meti-quits-over-sex-scandal-allegations/story-xdMnYjddeLdSfAurPMOETL.html>. (Accessed on 23 September2021).

[80] Amrit Dhillon, "Renu Mondal: Beggar Sings her Way to Bollywood," *The Times* (September 21, 2019), <https://www.thetimes.co.uk/article/renu-mondal-beggar-sings-her-way-to-bollywood-tvkhk7dtm>. (Accessed on 23 September 2021).

[81] Hans Graux, Jef Ausloos & Peggy Valcke, "The Right to be Forgotten in the Internet Era," in The Debate on Privacy and Security over the Network: Regulation and Markets 93, 94 (Jorge Pérez et al., eds., 2012).

the internet, even 'ordinary' folks were able to do so.[82] This is the most "likely to justify delisting" category since the individual in question is a "ordinary person" with no role in public life.

D. The relevance of the personal data to the public

The Data protection Committee Report, elaborates on what is meant by relevance of data to public as "whether the passage of time or change in circumstances has modified such relevance for the public."[83] The reason for providing such right is that often as time passes, a piece of information may become redundant or the information might become relevant to the public again. Accordingly, it's necessary to prevent certain piece of personal data from being removed.

The best example of these is *Google Spain* case[84] where due to the heavy debt incurred by Mr. Gonzaleza forced sale of property was conducted. Mr. Gonzalez succeeded in his claim that since the sale was conducted some 20 years ago it was no longer of much relevance. The decision was heavily criticised as critics claimed that giving preference to Mr Gonzalez's privacy right over the right of others is not justified.[85]

There draft bill doesn't establish a particular time period after which the personal data becomes irrelevant. This is perhaps because sometimes even a time lapse of 20 years is not enough to render the personal data relevant to public but a crime committed 2-3 years ago might make the personal data relevant. Thus, what is important to consider is the relevance of personal data and how it impacts the society. For instance, A Indian born US citizen accused and later got acquitted on a charge filled under the Narcotics Drugs and Psychotropic Substances Act, 1985 in 2009is justified in seeking delisting as not only charges made against him redundant today given his sober and healthy lifestyle but also because dismissal of delinking request would cause "irreparable Prejudice" to the Petitioner's career prospects.[86] Another instance could be of an accused though acquitted, the descriptive acquittal order was capable of creating bias in the minds of prospective employers.[87] However, a

---

82 Koops, *supra* note 62 at 236.

83 Data protection Committee Report, *supra* note 6 at 78.

84 *Google Spain case*, ECLI:EU:C:2014:317 (2014).

85 Amanda Cheng, *Forget About the Right to be Forgotten: How About a Right to be Different*, 22 AUCKL. Univ. Law Rev. 106, 119 (2016); Martin Husovec, "Should We Centralize the Right to be Forgotten Clearing House?" (2014), <http://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house> (Accessed on 24 September 2021); Rosen, *supra* note 2.

86 *Jorawer Singh Mundy* v. *Union of India*, 2021 SCC OnLine Del 2306.

87 *ABC* v. *Union of India*, Writ Petition 3499 of 2022 of Bombay High Court.

criminal charged with crime of sexual violence may not be able to make a successful delinking claim if his allows him to enter private homes.[88]

E. The nature of the disclosure and of the activities of the data fiduciary

This condition like the condition (3) discussed above acknowledges the need to balance between competing social interests. However, while condition (3) aims to balance the right to restrict the flow of information of aggrieved individual and the right to freedom and speech of third-party, this condition is specifically offered to balance individual's right to privacy against media's freedom of speech and expression.

Against the backdrop of right to be forgotten, Sec 20 of the draft bill expounds two concurrent considerations to be considered by the adjudicating authority when trying to balance the conflicting rights:

a) "Whether the data fiduciary "systematically facilitates" access to personal data, and

b) Whether any restriction on disclosure "significantly impedes" data fiduciary's activity."[89]

Thus, prima facie test is to determine whether an individual who "systematically facilitates" access to personal data (that is, journalist) and would be "significantly impacted" at the loss if disclosure of personal data is restricted.

i. Systematic facilitation

According to Data protection committee, "systematic facilitation" refers to the frequency of publication and economic necessity of conducting journalistic activity to the journalist.[90] For instance, individual who habitually use social media to post personal information to spread awareness about matters of public interest is different from individual that merely posted the picture of their friend's missing child to spread awareness of the possible kidnapping. Here the former can claim to be a journalist but latter cannot.[91]

---

[88] Google, The Advisory Council to Google on the Right to be Forgotten (4.4) (February 6, 2015), <https://archive.google.com/advisorycouncil/>. (Accessed on 23 September2021).

[89] The Personal Data Protection Bill, 2019, S. 20 (3)(*e*).

[90] The Committee of Experts on a Data Protection Framework for India, A Free and Fair Digital Economy Protecting Privacy Empowering Indians, 75 (2018), https://www.meity.gov.in/content/data-protection-committee-report (Accessed on 24 September 2021).

[91] Paulan Korenhof & Bert-Jaap Koops, "Identity Construction and the Right to be Forgotten: The Case of Gender Identity," in *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* 102, 119 (Alessia Ghezzi et al. eds., 2014).

Ostensibly, the criterion of "systematic facilitation" is extended because in recent times individual use not just traditional method of news dissemination such as newspapers and televisions but also non-traditional medium such as social media to disseminate information.[92] By proffering "systematic facilitation" as a criteria draft bill acknowledges that individual who publish certain content on social media networks such as Twitter and Facebook, could be considered as Journalists.

However, "systematic facilitation" is not final test to determine who is journalist. Instead, as data committee elsewhere notes, certain additional factors including social necessity of journalist's work and ethical standard of conduct of journalist should also be considered.[93] Therefore, the data protection committee leaves the door quite open in terms of factors necessary to decide who is a journalist.

ii. Significantly impediment

As noted, to claim protection against a claim of right to be forgotten, it's necessary to determine whether person who facilitated the dissemination of individual's personal data would be "significantly" impaired by the restriction on disclosure. The data protection committee is not clear on what constitutes as "significant impediment"; is there a degree of impediment necessary to be observed to constitute as significant? If so how is that degree established? Is the impediment here refers to economic impediment t, social impediment, cultural impediment or merely reputational impediment? All these questions must be settled.

IV. CONCLUDING REMARKS

The paper aims to study of how the draft bill attempts to solve the possible collision that emerges in context of social media, between right to be forgotten and other fundamental rights such as right to information or right to expression. Consequently,5-point criteria for balancing the conflicting rights provided in the bill has been analysed. The analysis as result indications certain limitations presents in the bill:

1. The bill provides for a household exemption but doesn't provide the set of standards necessary to determine the cases where such exemption would apply. The rationale is that cases would develop over time but in any case, certain minimum standards are necessary.
2. The definition of person who plays public role is problematic. According to the bill, public figure is someone who is either publicly

[92] Megan Knight, "Journalism as Usual: The Use of social media as a Newsgathering Tool in the Coverage of the Iranian Elections in 2009," 13(1) J. Media Pract. 61, 63 (2012).

[93] Data Protection Committee Report, *supra* note 6 at 143.

recognisable or he/she serves in public office. The bill affords them same standards even though a person who holds public office has higher responsibility to public. Also, certain extra conditions must be kept in mind while determining the public role. Such as waiver of right to privacy (that is deliberate disclosure) by the individual and Spectrum of publicity. Another study could be undertaken to determine whether the "reasonable expectation of privacy" test found in the English jurisprudence can be applied in India.

3. The draft bill establishes that individual who "systematically facilitates" access to personal data and who would be "significantly" impaired could have strong claim against right to be forgotten request. However, it does not define what could be considered as "significant impediment." Thus, certain criteria to distinguish between impediment and significant impediment must be laid down under the bill.

The paper here is however restricted in its scope a further extension of this research could be made in form of comparative analysis of the right to be forgotten present in different jurisdiction to determine if the solutions to the problems can be gathered form there. Also, the manner in which social media disseminates information changes rapidly. Another way of extending the research could be to extend the study into the technology dimension.