THE ORIGINS, JURISPRUDENTIAL FALLACIES AND PRACTICAL LIMITATIONS OF A 'RIGHT TO BE FORGOTTEN' IN THE EUROPEAN UNION

*Anujay Shrivastava**

Law Graduate (Class of 2020) from Jindal Global Law School,
O.P. Jindal Global (Institution of Eminence Deemed To Be University), Sonipat.
Email: 15jgls-ashrivastava@postjgu.edu.in

Abstract:

In the 21st century, an era dominated by internet and ever-expanding digitalization, it is difficult to hide electronic-footprints and information about ourselves from the world. In this regard, the emergence of a 'new' right to be forgotten (RTBF) in the EU, which protects the 'personal data' of individuals, has received critical acclaim. While tracing the origins, nature and scope of the RTBF in EU, this article shall attempt to best jurisprudentially locate RTBF as both an 'independent right' and a facet derived from values like 'privacy', 'autonomy' and 'dignity'. Subsequently, the problem of 'theoretical indeterminacy' arising from co-existence of RTBF and right to 'privacy' shall be addressed. Moving forward, the practical limitations of RTBF and its 'balancing' with competing rights/interests shall be delineated. Finally, a comparative analysis of the RTBF in the supra-national EU with the nascent development of RTBF and right to 'informational privacy' in India shall be undertaken.

Keywords: Controller/Operator, Data Subject, GDPR, Indeterminacy, Information, Right to Erasure (RTE), Right to be Forgotten (RTBF), Personal Data, Privacy, Processing

1. Introduction

The renowned Pulitzer Awardee and German-American psychoanalyst, E.H. Erikson was quoted saying that, "*In the social jungle of human existence, there is no feeling of being alive without a sense of identity*." [emphasis mine].[1] Erikson conveys the idea that a sense of *identity* is at the crux of

*I am indebted to Professor (Dr.) Alexander Christoph Fischer, for his valuable guidance and inputs on this journal article. Special thanks to Mr. Abhijeet Shrivastava, Mr. Anirban Chanda, Advocate (Mr.) Anubhav Khamroi, Professor Devyani Tewari, and Advocate (Mr.) Jayant Malik for providing feedback on an earlier draft of this article. Additionally, I am grateful to Professor (Dr.) Pritam Baruah, Professor Sachin Dhawan Esq., Ms. Aarushi Mishra, Ms. Akruti Ramachandra Chandrayya, Mr. Apoorv Madan, and Ms. Krishna Aarti Reddy, for insightful discussions in past concerning themes on privacy law and/or right to

being alive in our human existence. Sustenance of identity is the filament of life.[2] The desire to have *freedom* of living shapes our *identity*.[3] As humans, an intelligent species who self-identify as a 'social-animal', our identity comprises of various aspects which form an integral part of our life. These aspects include information about an individual's age, nationality, culture, sex, gender, sexuality, race, religion, caste, social-status, economic-status, physique, genetic data, mental health, education, criminal records, pending litigations, institutional affiliations, life achievements, and countless other things. Information corresponding to any of these aspects portrays a certain facet of our identity and inescapably forms a part of what one calls 'personal data' or 'personal information'.

Scholars have often stated that *personal data* is protected by the value of 'privacy', which exists today known as 'right to privacy', widely recognized as both a human right and a constitutional right.[4] The conceptualizations of right to privacy include the "accessibility-based" theory of privacy[5] and the "new definition" of privacy vis-à-vis undocumented personal data by authors such as Parent.[6] Scholars have also argued that privacy is a 'bundle of rights'[7] and encompasses numerous forms including 'zonal privacy',

---

be forgotten. I would also like to acknowledge my family and friends who have supported me throughout, especially during the difficult phase of the global COVID-19 pandemic. Views are strictly personal and do not constitute any advice or opinion, legal or otherwise. I reserve the academic freedom and the right to depart from these views in future.

[1] Erik H. Erikson, Identity: Youth And Crisis 68, W.W. Norton & Company (1968).

[2] *See Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1, ^3 (Dipak Misra, C.J.I. & A.M. Khanwilkar, J.) (*hereinafter* Navtej).

[3] Id.

[4] W.A. Parent, *Recent Work on the Concept of Privacy*, 20(4) American Philosophical Quarterly 341-355 (1983) (*hereinafter* W.A. Parent); Roger Ingham, *Privacy And Psychology* in John Young, Privacy 35-7, John Wiley and Sons (1978) (*hereinafter* Ingham); Richard Posner, *A Definition of Privacy*, 27 Rutgers Law Review 275 (1974) (*hereinafter* Posner); Anubhav Khamroi & Anujay Shrivastava, *Analysing The Practical Implications Of A Right to Privacy: State Surveillance And Constitution*, 8 Indian Constitutional Law Review 97-116 (2019) (*hereinafter* Khamroi and Shrivastava); Anubhav Khamroi & Anujay Shrivastava, *The curious case of Right to Privacy in India*, 2:12 Indian Constitutional Law Review 1-18 (2017) (*hereinafter* ICLR).

[5] *See* Ingham, *supra* note 4, p. 35-7; Posner, *supra* note 4, p. 275-96; Irwin Altman, *Privacy? A Conceptual Analysis*, 8 Environment and Behavior 7-29 (1976) (*hereinafter* Altman). For further reading, *see also* W.A. Parent, *supra* note 4, 341-355; Khamroi and Shrivastava, *supra* note 4, p. 104.

[6] W.A. Parent, *supra* note 4; Khamroi and Shrivastava, *supra* note 4, 104-5.

[7] Jon L. Mills, Privacy: The Lost Right 4, Oxford University Press (2008); Judith Jarvis Thomson, *The Right to Privacy*, 4 Philosophy and Public Affairs 295-315 (1975); Ernest Van Den Haag, *On Privacy*, in Privacy, Nomos XIII: Yearbook Of The American Society For Political And Legal Philosophy 149, Atherton Press (1971); Leslie Regan Shade, *Reconsidering the Right to Privacy in Canada*, 28(1) Bulletin of Science, Technology and Society (2008); Khamroi and Shrivastava, *supra* note 4, 102.

'relational privacy' and 'decisional privacy'.[8] In light of the developing scholarship, privacy encompasses and protects a wide range of actions in both public and privates spheres of an individual's life, including their personal data. However, authors such as Khamroi and Shrivastava have disagreed with the proponents of the 'bundle of rights' theory, arguing that privacy has gone through *theoretical incoherence* and constantly evades the trap of a singular definition.[9] They argue that other constitutional/human values such as liberty, autonomy and dignity provide agency to an individual to perform certain private acts, without any external interference from the state or other external individuals. Consequently, they state that privacy is needed as an *independent right* to protect both *documented* and *undocumented* personal data.[10]

The evolving global jurisprudence in the 21st century era, has given rise to discussions on a new right, notoriously dubbed as "*derecho al olvido*" (Spanish phrase)[11], which is more famously known as the "Right to be Forgotten" (*hereinafter* **RTBF**) or "Right to Erasure" (*hereinafter* **RTE**). Scholars[12] claim that this right was first acknowledged or created in the European Union (*hereinafter* **EU**) by an international judicial-body in *Google Spain*[13], which was a decision delivered by the Grand Chamber of the Court of Justice of the European Union (*hereinafter* **ECJ**). Indeed, prior to the digital age of internet, the very existence of RTBF/RTE, as recognized by the EU Law and later nations abroad could not have been

[8] ICLR, *supra* note 4, 1-18; Anujay Shrivastava, *Reconstructing the Decisional Paradigm of Privacy: Crafting a new Anti-Manifesto Grounded on Shadows of The Enabling School*, 6 Indian Constitutional Law Review 7-23 (2018).
[9] Khamroi and Shrivastava, *supra* note 4, 97-8; ICLR, *supra* note 4, 1-2.
[10] Khamroi and Shrivastava, *supra* note 4, 105-6.
[11] *See* Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Request for a preliminary ruling from the Audiencia Nacional.)*, ECLI:EU:C:2014:317: ILEC 060 (ECJ 2014), ^20, 91 (*hereinafter* Google Spain). This important decision, which will be substantially discussed in later parts of this article, mentions RTBF only twice. For a greater perspective into initial academic writings on RTBF prior to the *Google Spain* decision, *see* Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012); Jef Ausloos, *The 'Right to be Forgotten' – Worth remembering?*, 28(2) Computer Law & Security Review 143 (2012); Steven C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, 30 Berkeley J. Int'l L. 161 (2012); Robert Kirk Walker, *The Right to be Forgotten*, 64 Hastings L.J. 257 (2013).
[12] Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, The Right To Be Forgotten, And The Construction Of The Public Sphere*, 67 Duke Law Journal 981-2 (2018); Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, 14(4) Human Rights Law Review 761-77 (2014); Prashant Mali, *Privacy Law: Right To Be Forgotten In India*, 7 NLIU Law Rev. 7-21 (2018) (*hereinafter* Mali).
[13] Google Spain, *supra* note 11.

ever imagined. Mali asserts that RTBF/RTE should be understood as an individual claim where the individual has the power to 'delete' or 'erase' personal data in order to ensure that such personal data cannot be traced by any third parties.[14] RTBF extends protection not only to the personal data of individuals (such as data shared on a social-media account or an online diary), but principally accords protection to an individual's identity and the individual themselves.

The emergence of RTBF/RTE in EU and nations abroad has received praise from both academia, legal practitioners and ordinary people as a remarkable development which has provided a legal framework and recognized right that can protect an individual's personal data. In fact, the General Data Protection Regulation[15] (*hereinafter* **GDPR**), has been hailed by journalists and scholars alike as the world's toughest and most comprehensive framework to protect personal data.[16] However, whether RTBF/RTE should be considered a right in its own self or whether it is a facet of other constitutional/human values such as privacy or dignity are both strongly contestable claims. Moreover, even if we assume that RTBF is a right in its own self, it is unclear where should we place it in the realm of human rights or constitutional rights, given the fact that personal data (whether documented or undocumented) is already covered or protected by conceptions of privacy.

With this prelude, the first segment of this article shall trace the origins of RTBF in the EU through analysis of the *Google Spain* case and the relevant EU legislations. In this segment, I shall lay down what are the exact contours of this right and its scope. Subsequently, the second segment shall examine various theoretical positions from which RTBF (*as it exists today in EU Law*) can be jurisprudentially traced. This segment shall discuss whether RTBF is a facet of constitutional/human values such as privacy, autonomy and dignity, or is RTBF an independent right/value. Moving on, the third segment shall discuss whether the existing jurisprudence governing RTBF in the EU leads to theoretical indeterminacy. The fourth segment shall discuss various limitations of RTBF and its balancing with competing interests, including discussions on commercial surveillance and commercial

[14] See Mali, *supra* note 12, 7-21.

[15] 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 (General Data Protection Regulation), May 5, 2016, OJ L 119, 1–88 (European Union) (*hereinafter* GDPR).

[16] Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR.EU, available at: https://gdpr.eu/what-is-gdpr/ (Last Visited on May 25, 2021); Federico Fabbrini & Edoardo Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, 21 German Law Journal, 55–65 (2020).

interests, state surveillance and public interests, and potential chilling effects on competing rights/interests. Finally, the last segment shall engage in a comparative analysis of RTBF in the multi-national EU with India, and share some insights into similarities or differences on a RTBF framework in the two jurisdictions. In the Concluding Remarks, I shall highlight important considerations regarding RTBF for both the jurisdictions of EU and (especially) India, as well as reflect on the jurisprudential fallacies of the RTBF in the EU.

2. The European Union and the RTBF/RTE

In this segment, I shall examine the development of RTBF/RTE in the EU. *First*, I shall look at the relevant EU legislations prior to the *Google Spain* decision which govern personal data and its interaction with an individual's human right to privacy. *Second*, I shall examine the relevance of the ECJ's *Google Spain* decision. *Third*, the RTBF shall be discussed in light of the GDPR. *Last*, I shall discuss contemporary developments succeeding the *Google Spain* decision.

2.1. Legislative origins of RTBF in the EU: Pre-GDPR Developments

The most important authority in EU Law on privacy is enshrined in Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms (*hereinafter* **ECHR**), which provides an individual the right to respect of their *private life*.[17] This is a limited right and public authorities may curtail or interfere with this right under certain situations.[18] Importantly, ECHR was formulated in an era where internet, social media and digital storage did not exist. Owing to lack of advancement in the technology, it is inconceivable to believe that 'personal data' was intended to be covered and protected by the ECHR. The ECHR as it stands today has no mention of RTBF even after its amendments from protocols nos. 11 and 14, as well as supplements by protocols nos. 1, 4, 6, 7, 12 and 13. Consequently, personal data was not originally intended to be covered under right to privacy and its forms.

With that prelude, lets venture into the origins of RTBF/RTE in the EU. Directive 95/46 of the European Parliament[19] (which now stands repealed by the GDPR), defines 'personal information' as:

[17] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, art 8(1) (*hereinafter* ECHR).
[18] *See id*., art 8(2).
[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the

> "…*any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"* [emphasis mine][20]

Remarkably, the above-mentioned definition also defines and utilizes the concepts of a 'data subject', as well as provides various factors (including an identification number) which allow anyone to identify an individual (whether directly or indirectly) by possessing that information. Directive 95/46 also presents a broad and expansive definition of actions which constitute what is called 'processing' (whether automatic or non-automatic) of *personal data*.[21] For illustration, actions such as collection, recording, organisation, storage or use of personal data, are all covered by the definition of processing. Moreover, processing of personal data (*which forms or intends to form a part a filing system*) by automatic means, partly-automatic means or non-automatic means are all covered under Directive 95/46.[22] At this juncture, it is important to note that Directive 95/46 does not expressly mention or discuss RTE/RTBF.

The ECJ in *Google Spain* decision had recorded that the objective of Directive 95/46 is to "*protect the fundamental rights and freedoms, notably the right to privacy, of natural persons*" [emphasis mine]. This right to privacy would cover any action constituting processing of personal data.[23] Moreover, Directive 95/46 itself records that "*data-processing systems are designed to serve man*" and must respect their fundamental rights and freedoms (irrespective of nationality or residence of natural persons), especially their right to privacy.[24] Bound by Directive 95/46, the national laws of various EU states which regulate *processing* of personal data, pursue the objective of protecting the right to privacy of data subjects as recognized by ECHR and the general principles of community law.[25] Consequently, by the passage of Directive 95/46, the EU legislatively expanded the scope of right to privacy to extend to protecting 'personal

---

free movement of such data, November 11, 1995, OJ L 281, 31–50 (European Union) (*hereinafter* Directive 95/46).

[20] *See id*., art 2(a).

[21] *See id.*, art 2(b).

[22] *See id.*, art 3(1).

[23] *See* Google Spain, *supra* note 11, ^58, 66.

[24] *See* Directive 95/46, *supra* note 19, recital 2. The readers may bear in mind that while recitals are not the applicable/enforceable provisions of EU legislations, they are treated as an interpretative guide while understanding a EU Directive or EU Regulation.

[25] *See id*., recital 10.

data' of individuals. Indeed, the EU Parliament intends for every EU member state to have its own law on processing of personal data, so that individuals are not deprived of the protection to which they are entitled to under the expanding scope of right to privacy based on Directive 95/46.[26] The emphasis on data protection is so strong, that processing of data carried out by legal persons established in a third country (i.e., a non-EU country), which bear some relation to a EU member state (such as actions of parent companies abroad which have a subsidiary company in an EU member state), must not stand in the way of privacy rights guaranteed under Directive 95/46.[27] Consequently, each EU member state has to mandatorily adopt a national law to regulate and govern processing of personal data, especially to address situations where the means to process personal data are located within that EU member state. Importantly, the Directive 95/46 imposes certain important positive obligations concerning personal data on both the EU Member State, as well as the "controller"[28], which they both have to ensure fulfilment of.[29] However, the controller is empowered to ensure direct compliance with obligations provided under Article 6(1) of Directive 95/46.[30]

Subsequent to adoption of Directive 95/46 by the EU Parliament, every EU member state was obligated to mandatorily adopt a national law, ensuring effective compliance with obligations to protect the right to privacy of individuals.[31] The national laws adopted by the EU member states must reflect the principles for protection of an individual's right to privacy, which impose obligations on legal persons who are responsible for processing various aspects related to personal data. Moreover, such legal persons have a duty to inform the individuals protected under Directive 95/46, whenever their personal data is being processed. The individuals have right to be allowed to 'consult the data', to 'request corrections' and even to 'object to processing' of that data in *certain circumstances*.[32] This includes the right to limit access, restrict usage or even seek erasure or deletion of the personal

[26] *See id*., recital 20.
[27] *See* Directive 95/46, *supra* note 19, recital 19. This obligation has been reiterated by the ECJ, *see also* Google Spain, *supra* note 11, ^48.
[28] *See generally* Directive 95/46, *supra* note 19, art 2(d). (Directive 95/46 had provided an extensive definition of a "controller", who essentially had power to jointly or alone determine the purposes and means of processing personal data. If the EU member states were empowered to determine by national law or principles of community law in the EU, the purposes and means of 'processing', they could also determine who would be designated as the controller and lay down the specific criterion to nominate them.)
[29] *See id*., art 6.
[30] *See id*., art 6(1), 6(2).
[31] *See id*., art 4.
[32] *See id*., recital 25.

data.[33] However, the rights of these individuals, as evinced from the phrase "certain circumstances"[34] in Recital 25 of Directive 95/46, implies that their rights are restricted/limited in nature. Consequently, one could argue that this protection can be understood as a limited RTBF with a very restrictive scope under the EU Law. Alternatively, as proponents of privacy would argue, the protection in Directive 95/46 could be logically seen as a positive obligation arising out of the individual's *right to privacy* under the EU Law and *general principles of EU community law*.

2.2. Case Study: Google Spain

The *Google Spain* decision by the ECJ was the first instance in EU, where an international court had expressly mentioned the RTBF/RTE, although it did not elaborate significantly on the concept.[35] Almost entirety of the *Google Spain* decision discusses the right to privacy and protection of personal data.

Prior to delving into the *Google Spain* decision's rulings, it is essential to advert to brief facts of the case. A Spanish citizen, *Mario Costeja Gonzalez* (complainant), had lodged a complaint under the *Agenda Espanola de Proteccion de Datos* (AEPD), which is the Spanish Data Protection Agency. The complainant wanted deletion of an old link to a newspaper article regarding a real estate auction that had taken place for the recovery of his debts. The complaint was made against *La Vanguardia Ediciones SL* (news publisher), a news publisher based in Spain that published the news about the complainant and the real estate auction in both hard-copy and an online medium during 1998. Google Spain and Google Inc. (*hereinafter*, collectively referred to as "Google Collective") were also made a part of the complaint. Google Collective had displayed the link to the above-mentioned articles in its search platform, i.e. Google's results, whenever the name of the complainant was entered.[36] The AEPD rejected complainant's claim against the news publisher, as the publication of the news was done in accordance with a national court order. However, the AEPD allowed the complainant's request against Google Collective, directing Google Spain to remove the display of links to the news publisher's articles from its search results.[37] The AEPD recorded that under Directive 95/46 and general principles of EU community law, the complainant had a right to privacy, which would be violated should the Google companies continue to display the link in their search tool results, even if it was being done lawfully. The

[33] *See id*., art 2(b).
[34] *See id*., recital 20.
[35] *See* Google Spain, *supra* note 11, ^20.
[36] *See id*., ^1-2, 14-20.
[37] *See id*., ^2.

force of the complainant's rights under the directive had greater weightage than Google's lawful act of presenting the search results.[38]

Subsequently, the companies of Google Collective brought separate actions against the EPD decision before the *Audiencia Nacional* (National High Court), Spain, which were clubbed together. The National High Court referred certain questions of law regarding interpretation of Directive 95/46 to the ECJ.[39] Moving forward, the ECJ started its analysis by observing that the activity of a search engine such as Google (which is owned by Google Collective), as a provider of content which consists in "*finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference*" needs to be classified as *processing* of *personal data* within the meaning of Article 2(b) of Directive 95/46.[40]

The ECJ recorded that the operation of loading personal data on an internet page must be considered to be such *processing*[41], even when such action concerns material which has been *lawfully* published in an unaltered form.[42] Should the national authorities or ECJ not include Google Collective's actions within the ambit of *processing* of personal data, the objective of Directive 95/46 would fail.[43] Moreover, since Google Collective (i.e., the operator of the search engine) is the person responsible for determining the purposes and means of the activity (i.e. the processing), the Google Collective is bound to ensure that the processing of personal data meets the requirements of Directive 95/46. The ECJ added that this was to ensure that the fundamental right to privacy of the data subjects is protected, as well as effective and complete protection of personal data covered within the foregoing right is achieved.[44] It further recorded that the scope of definitions under Article 2 of Directive 95/46 cannot be interpreted restrictively, when the effective and complete protection of the fundamental rights and freedoms (especially the right to privacy) of individuals is to be ensured.[45]

---

[38] *See id*., ^81, 97.
[39] *See id*., ^20.
[40] *See id*., ^28.
[41] *See id*., ^25.
[42] *See id*., ^30. The ECJ placed reliance on its earlier decisions in Lindqvist and Satakunnan, *see* Case C-101/01, *Lindqvist*, ECLI:EU:C:2993:596, ^25 (ECJ); Case C-73/07, *Satakunnan Markki naporssi and Satamedia*, EU:C:2008:727, ^48-49 (ECJ).
[43] *See* Google Spain, *supra* note 11, ^34.
[44] *See id*., ^38.
[45] *See id*., ^53. The ECJ relied on an earlier precedent in L'Oreal, *see* Case C-324/09, *L'Oreal and Others*, EU:C:2011:474, ^ 62-63 (ECJ).

Subsequently, the ECJ recorded that in order to comply with the provisions of Directive 95/46, the operator of a search engine is under legal obligation to remove the links to the articles (which includes personal data of the complainant) from its search results. The operator would be under the foregoing legal obligation, when search results are displayed following a search made on the basis of a person's name, which display web links to web-pages mentioning the person's name and personal data, or when links to web-pages published by third parties contain information relating to that person, or where the name or information is not erased beforehand or simultaneously from such web-pages, or even when its publication in itself on those web-pages is lawful.[46] However, the ECJ clarified that this is not an absolute obligation. The conditions specified in Article 7(1) read harmoniously with Article 12 and Article 14 of Directive 95/46 need to be met in order for the operator to comply with the complainant's request.[47] At the same juncture, it must be borne in mind that Directive 95/46 seeks "*to ensure a high level of protection of the fundamental rights and freedoms of natural persons*", especially their 'right to privacy' in respect of processing of personal data.[48] The ECJ also recorded that the provisions of Directive 95/46 must be interpreted in light of fundamental right to privacy, which forms an integral part of EU Law.[49]

Importantly, the ECJ held that without prejudice to specific provisions that the EU member states may set out in their national law in respect of processing for 'historical', 'statistical' or 'scientific purposes' (as per exceptions to Article 6 of Directive 95/46):

> "*the **controller** (herein Google Collective) has the task of ensuring that personal data are **processed 'fairly and lawfully'**, that they are **'collected for specified, explicit and legitimate purposes** and **not further processed in a way incompatible with those purposes'**, that **they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'**, that **they are 'accurate and, where necessary, kept up to date'** and, finally, **that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'**. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified."*[50][emphasis mine]

[46] *See id*., ^62.
[47] Id.
[48] Id.
[49] *See id*., ^68.
[50] *See id*., ^62.

As per the above quotation, it is important to note that these obligations all arise from the provisions of Directive 95/46. Therefore, the ECJ is not going beyond what is expressly provided by the EU Parliament in the express language of Directive 95/46.

In relation to the *Google Spain* case, the ECJ recorded that the operator of a search engine (Google Collective) is liable to significantly affect "*the fundamental right to privacy and protection of personal data, when the search by means of that engine is carried out on the basis of an individual's name*." The processing by an internet search engine enables anyone to obtain a structured overview of the information relating to the data subject (complainant) that can be found on the internet, through the list of results from the search engine. The information on the internet potentially contains a vast number of the complainant's private life. This sensitive information, which could have otherwise not been interconnected or interconnected with great difficulty without obtaining the search engine's results. Therefore, the search results allow any individual or legal persons to establish a detailed profile of the complainant.[51] Moreover, the effect of the "*interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in the modern society, which render the information contained in such a list of results ubiquitous.*"[52]

Ultimately, the ECJ held that the operator of a search engine is obligated to remove the links to web-pages that contain "*information relating to the data subject published by the third parties*", where a search made on the basis of an individual's name corresponds to information publicly uploaded on such web-pages. Moreover, the search results showing links containing information relating to the data subject in cases where, [i.] the name or information is not erased beforehand, or [ii.] is simultaneously obtained from such web-pages, or [iii.] even when the publication in itself on those web-pages is lawful, can be ordered to be removed by the operator.[53] Having regard to the sensitivity of the complainant's information (especially their private life) contained in the announcements provided in the original article and the fact that the initial publication had taken place nearly two decades earlier, the ECJ held that the complainant had established a right that "*the information should no longer be linked to his name by means of such a list*."[54]

[51] *See id*., ^80.
[52] Id.
[53] *See id*., ^88.
[54] Id.

However, the ECJ also read in limitations and pre-requisites to this right under the Directive 95/46. As the Directive 95/46 stands repealed, the ECJ's limitations and pre-requisites are not binding in light of data protection framework introduced by the GDPR. Nonetheless, we shall be discussing them later in context of analysing whether RTBF is an independent right in Part 3.1.[55]

2.3. The GDPR Regime

The GDPR was adopted by the EU Parliament after the ECJ's *Google Spain* decision. As stated earlier, the GDPR repealed Directive 95/46 and was its successor in the objective of protecting personal data. It has been transposed into the national laws of twenty-eight members of the EU (including the United Kingdom, prior to its exit from the EU). Moreover, at least five nation states which are candidates to be future members[56] of the EU are in the process of transposing the GDPR into their own national laws, as a pre-requisite to become an EU member state.

The GDPR expands the definition of a data subject.[57] Article 9(1) of the GDPR also prohibits processing of 'special personal data' of a data subject, such as information which can reveal their race, ethnic origin, political opinions, religion, philosophical belief or membership of a trade union.[58] Moreover, the processing of 'genetic data' or 'biometric data' for the purpose of uniquely identifying a natural person, or information concerning their health, sex life or sexual orientation is prohibited under Article 9(1).[59] However, there are various exceptions to the above-mentioned prohibitions on processing certain information/data.[60] Nonetheless, the fact that such prohibitions are encompassed by the GDPR demonstrate how progressive and privacy-friendly the EU regulation is.

Article 17 of the GDPR provides a right to a data subject, to seeking erasure of personal data related to them by the "controller"[61], without undue delay.[62] Importantly, Article 17 is titled "Right to erasure ('right to be forgotten'), encompassing both RTE and RTBF. This provision provides for six broad

[55] *See* discussion *infra* Part 3.1.
[56] *Countries | European Union*, European Union, available at: https://europa.eu/european-union/about-eu/countries_en#tab-0-1 (Last Visited on May 25, 2021).
[57] *See* GDPR, *supra* note 15, art 4(1).
[58] *See id*., art 9(1).
[59] Id.
[60] *See id*., art 9(2).
[61] *See id*., art 4(7).
[62] *See id*., art 17.

grounds on which erasure of data can be sought by a complainant (see quotation below):

> "*1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
> *2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) [the data subject has given consent to the processing of his or her personal data for one or more specific purposes], or point (a) of Article 9(2) [the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 (Article 9(1)) may not be lifted by the data subject], and where there is no other legal ground for the processing;*
> *3. the data subject objects to the processing pursuant to Article 21(1) [general right to object] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
> *4. the personal data have been unlawfully processed;*
> *5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
> *6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*" [emphasis mine][63]

Greater context on RTBF can be found in Recital 65 and Recital 66 of the GDPR.[64] Remarkably, the recitals in the GDPR are a rare example of employing a feminist style of drafting when mentioning individuals (such as use of the word 'her' instead of 'his'), which is appreciable for a multi-nation state regulation adopted by the EU Parliament. As per Recital 65, a data subject should have the RTBF over *her* personal data, where the retention of such data infringes the GDPR, EU Law or a law of an EU member state. Importantly, this recital pays great emphasis on *consent* of the data subject.[65] The recital also states that RTBF is relevant where the data subject may have given her consent "*as a child, is not fully aware of the risks involved by the processing of her data then, and later wants removal of such personal data, especially on the internet.*"[66] This remarkably makes GDPR the first EU legislation to provide for protection of personal data in response to the growing threats by the internet. Moreover, Recital 66

[63] Id.
[64] *See id*., Recital 65.
[65] Id.
[66] Id.

expressly states that in order to strengthen the RTBF in the online environment, the 'right to erasure' (RTE) (*which is a synonym for the same right, i.e. RTBF*) should be extended in such a manner, that any *controller* (who has made the personal data public) should inform the processing controller to erase any links to the personal data, or copies/replications of the personal data.[67] Clearly, Recital 66 mirrors the response of ECJ in the *Google Spain* case.

While RTBF has been expressly prescribed in Article 17(1), it is subject to multiple exceptions under Article 17(3). These exceptions include 'necessity' for exercise of right to freedom of expression and right to information, compliance with a legal obligation in public interest, public health, scientific or historical research, statistical purposes and establishment, exercise or defence of legal claims.[68] Importantly, a 'right to rectification' of personal data and a 'right to restriction of processing' have also been distinguished from RTBF/RTE in the GDPR, under Article 16 and Article 18 respectively. Consequently, the scope of RTBF/RTE has been restricted to only those cases where erasure of personal data is necessary.

2.4. Further Developments – Case Study: Google LLC

Following the adoption of the GDPR, the ECJ in the recent *Google LLC*[69] (2019) decision has ruled that an operator (Google LLC) is not bound to apply RTBF/RTE globally, but only in the member states of the EU. If a competent authority established under the national law of a EU member state determines that search engine results containing link to *personal information* of a person have to be removed by the operator of the search engine, then such an operator "*cannot be required to carry out a de-referencing on all the versions of its search engine*." The obligation on the operator to remove processing of personal data is restricted to only those search engine versions, which are corresponding to EU member states.[70] Consequently, the *territorial application* of the RTBF under EU law has been read to be restricted to only EU member states.

The ECJ did, however, record that while EU Law does not currently require that a de-referencing order to the operator made by a competent authority mandate removal of personal data from all versions of a search engine, such

[67] *See id*., Recital 66.
[68] *See id*., art 17(3).
[69] *See* Case C-507/57, *Google LLC (successor to Google Inc.) v. Commission nationale de I'informatique et des libertes (CNIL)*, ECLI:EU:C:2019:772, ^ 72-3 (*hereinafter* Google LLC).
[70] *See id.,* ^72.

a practice is not prohibited under the GDPR or the EU Law.[71] Thus, both supervisory or judicial authorities constituted under national law of member states retain the power to determine whether it is necessary to order de-referencing of personal data from all versions of search engines handled by an operator (such as Google), if it is necessary to give effect to the fundamental rights of a data subject under the GDPR.

3. Jurisprudential Origins of the RTBF/RTE: Revisiting Human/Constitutional Values

In the previous segment, we discussed the origins of RTBF/RTE in the EU. We also learnt about the scope of RTB/RTE in light of the GDPR and further developments in the *Google LLC* decision. In this segment, I shall attempt to explore the jurisprudential/theoretical origins of RTBF. I shall examine whether the RTBF can be considered as an independent right on its own. Alternatively, whether RTBF is a facet of other recognized human/constitutional values, *in particular*, privacy, autonomy and dignity. In order to maximize the theoretical discussion on the RTBF jurisprudence, a comparative approach while discussing jurisprudence and constitutional law will be utilized in the following sub-segments, in order to gain a better understanding of the various rights and constitutional values.[72]

3.1. RTBF and its scope as an 'independent right' on its own

While nations across the world have been expanding the scope of privacy to cover protection of personal data and some nations have considered adopting provisions similar to the RTBF in the EU, the current jurisprudence on RTBF is largely restricted to the EU. Under the EU jurisprudence derived from the erstwhile Directive 95/46 and *Google Spain* decision, it is inconceivable to conceptualize RTBF as an independent right on its own. As noted earlier, both the directive[73] and the *Google Spain* decision[74] permit for *erasure* of personal data due to the data subject's fundamental rights and freedoms envisaged in EU Law and general principles of community law, especially the *right to privacy*.

However, while it is theoretically inconceivable to conceptualize RTBF as an independent right or human value on its own, it can be established as a right by a statute or a legal instrument in a nation state. As noted earlier, the

[71] Id.
[72] *See* Ran Hirschl, *The Rise of Comparative Constitutional Law: Thoughts on Substance and Method*, 2 Indian J. Const. L. 12 (2008) (*hereinafter* Hirschl).
[73] *See* Directive 95/46, *supra* note 19. The relevant references include Articles 1 and 9, as well as Recitals 2, 10, 18-20 and 25 of the directive.
[74] *See* Google Spain, *supra* note 11, ^3, 38, 53, 58, 66, 74, 87.

GDPR which establishes a new data protection regime for the EU, expressly provides a limited RTBF/RTE in both its text and effective provisions. Almost every EU member state has its own national law which is *in pari material* with the GDPR. Similarly, the erstwhile Directive 95/46 in light of the *Google Spain* decision did also provide for limited circumstances when a data subject would have a RTBF. This shows us that legislative instruments, whether national or multi-national, can create a real and 'practical' RTBF.

Stemming from the discussions in the *Google Spain* decision, a question that comes to one's mind immediately is what would be the scope of the right or protection offered by RTBF, if it is an independent right? As recorded by the ECJ in *Google Spain*, the RTBF of a data subject emerging from Directive 95/46 would be limited and subject to restrictions.[75] Moreover, there would be a positive obligation on a controller under the EU Law and Directive 95/46 to ensure that the personal data is:

> "*1. Processed 'fairly and lawfully';*
> *2. Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;*
> *3. Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;*
> *4. Accurate and, where necessary, kept up to date;*
> *5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed; and*
> *6. Erased or rectified, taking every reasonable step, wherever the personal data does not meet the requirements of the provisions of Directive 95/46.*"[76]

The ECJ in *Google Spain* added an important pre-requisite, which needs to be met before examining whether the compliance of a controller's processing of personal data under the directive needs to be looked at. It stated that an examination of whether the data subject "at the present point of time" has a right to request delinking of personal information (information relating to data subject personally) that is displayed following a search made on the basis of their name, needs to be made by the concerned authority/controller.[77] Moreover, the ECJ recorded that it is not necessary to find out whether the inclusion of the information in question in the list of results causes prejudice to the data subject.[78]

[75] *See* Google Spain, *supra* note 11, ^62.
[76] Id.
[77] *See id*., ^96.
[78] Id.

Further, the ECJ held that the authority (while balancing the economic and other interests of the controller, as well as the interest of the general public in finding that information (right to information) upon a search relating to the data subject's name, with the subject's rights under the Directive 95/46) needs to consider the fact that the data subject's rights under the directive, as well as the fundamental freedoms and rights guaranteed under general principles of EU law are intended to override controller and general public's interests. However, if there appear to be particular reasons to make the personal data of the data subject publicly available, the authority may reject a data subject's claim for erasure or limitation of availability of their personal data.[79]

It is to be cautioned for the reader that the above-mentioned obligations arising from Directive 95/46 and the *Google Spain* decision are no longer effective, having been changed since the introduction of the GDPR (refer to Part 2.3).

3.2. RTBF as a facet of 'privacy'

As discussed in the previous section, while RTBF/RTE has been recognized and enforced by way of national or multi-national legislations (such as the EU Directives or Regulations), it is notable that as far as the EU jurisprudence is concerned, the RTBF stems from the existing "fundamental rights and freedoms" under the EU law. In fact, there is a consistent mention of right to privacy[80] in the Directive 95/46, which was first provided to citizens of EU member states by the ECHR and the general principles of EU Law. Consequently, it can be argued that the EU Law considers RTBF as a facet of right to privacy.

Previously, we have observed the limited scope of RTBF. The obligations provided to a controller are akin to the *accessibility-based* theorization of privacy.[81] The accessibility-based theory conceptualizes *privacy* as one's right to take away the ability of *others* to access or acquire their personal information. According to this theory, the mere possibility that others could acquire personal data would itself constitute a violation of the right to privacy, even where there is no attempt to acquire personal data.[82] The ECJ

[79] Id.
[80] *See* Directive 95/46, *supra* note 19. Refer to Articles 1 and 9, as well as Recitals 2, 10, 18-20 and 25 of the directive.
[81] Ingham, *supra* note 4, 35-7; Posner, *supra* note 4, 275-96; Altman, *supra* note 5, p. 7-29. For further reading, *see also* W.A. Parent, *supra* note 4, 341-55; Khamroi and Shrivastava, *supra* note 4, 104.
[82] *See* Altman, *supra* note 5, 7-29; W.A. Parent, *supra* note 4, 341-55.

in *Google Spain* had reached a similar conclusion, when it held that the mere possibility that an individual can have an easier access to the personal data of a data subject using Google's search results, was liable to significantly affect the fundamental rights to *privacy* and the protection of personal data.[83] As discussed earlier, the ECJ in *Google Spain*, noted that the personal data that concerns a vast number of aspects relating to a data subject's private life would be otherwise inaccessible or greatly difficult to find, unless the Google search results showed them immediately by just typing the name of the data subject.[84] The effect of the interference with the rights of the data subject is heightened by internet engines that render personal data *universally-available* using their search results.[85] The ECJ has acknowledged that the mere potential or possibility of interference with the rights of the data subject by acquiring the personal data can violate their right to privacy. Therefore, RTBF under the EU jurisprudence can indeed be understood as a facet of right to privacy (especially the accessibility-based theory of privacy).

However, this also leads us to a conceptual dilemma, when we understand the restricted scope of privacy and the protections provided by other human rights/fundamental rights/constitutional values such as dignity, liberty, autonomy etc. If we consider the scope of RTBF discussed earlier and the scope of right to privacy, we face a problem where scope of the two rights would look excessively similar and both protect personal data of an individual. Such a scenario leads to *theoretical indeterminacy* with regard to the scope of both right to privacy and RTBF. This theoretical indeterminacy shall be addressed in Part 4 of this article.

3.3. RTBF as a facet of 'autonomy' or the 'control-based' theories of 'privacy'

'Autonomy' which is considered as a constitutional value, a human right and in rare instances a fundamental right, provides protection to an individual from 'external interferences'.[86] Autonomy is not a synonym for 'dignity', which is a separate right or constitutional value, but a description of one of its attributes.[87] A simple understanding of individual autonomy

[83] *See* Google Spain, *supra* note 11, ^80.
[84] Id.
[85] *See* Google Spain, *supra* note 11, ^80; Joined Cases C-509/-9 and C-161/10*, eeDate Advertising GmbH and Others v X and Société MGN LIMITED*, EU:C:2011:685, ^45 (ECJ).
[86] Alan Westin, Privacy And Freedom 1-22 (1967). For further reading, *see* Khamroi and Shrivastava, *supra* note 4, 103.
[87] John A. Most, *Autonomy and Rights: Dignity and Right*, 11 J. Contemp. Health L. & Pol'y 473 (1995).

would be to say that "…*it is an idea that is generally understood to refer to the capacity to be one's own person, to live one's life according to reasons and motives that are taken as one's own and not the product of manipulative or distorting external forces*" [emphasis mine].[88] The 'control-based' theories of privacy which state that an individual should have 'absolute control' over their personal data and be able to share it at its own will[89], are similar to the value of autonomy. The control provided by *autonomy* to an individual would include the ability to prevent disclosure of "*personal information to individuals, other than those to whom one has voluntarily revealed it*."[90]

The RTBF within the realm of 'autonomy' and 'control-based' theory of privacy would provide the data subject as understood under the EU jurisprudence with near-absolute control over their personal data. Moreover, this would mean that any personal information that has been shared with regard to a data subject without their consent cannot be allowed. If we were to take such an understanding of RTBF in the *Google Spain* case, then in theory, the AEPD should have restricted even the newspaper publisher (even if it was done as per the order of the court) and not only Google Collective from publishing the information related to the data subject. Such an interpretation of 'RTBF' having arisen from 'autonomy' or 'control-based' theories of privacy would raise questions with regard to potential 'chilling effects' on other individuals' rights, state sovereignty vis-à-vis judicial institutions and the legitimate state interests of the EU member states.

While it is difficult to conceptualize 'RTBF' as a facet of 'autonomy' or the 'control-based' theories of privacy, it is indeed possible for such a position to eventually emerge by legislative/statutory enactments or evolving judicial-precedents. In Part 5.3 of this article, we shall see how the RTBF can be practically exercised in a way similar to its conception as a facet of autonomy or 'control-based' theories of privacy, as well as the potential of *chilling effects* created by it.

3.4. RTBF as a facet of 'dignity'

The famous dissent of Justice Frank Murphy in the landmark *Korematsu* decision by the Federal Supreme Court of United States, was one of the first instances where a court had invoked the constitutional value of 'dignity' in a

[88] John Christman, *Autonomy in Moral and Political Philosophy*, The Stanford Encyclopaedia of Philosophy, January 9, 2015, available at: https://plato.stanford.edu/entries/autonomy-moral/. (Last Visited on May 25, 2021).
[89] Khamroi and Shrivastava, *supra* note 4, 105.
[90] Id.

judicial decision. Justice Murphy condemned the majority opinion of the court as "*adopting one of the cruellest of the rationales used by the enemies of United States*" enemies to destroy the dignity of an individual.[91] Dignity is a well-established constitutional value in the modern world.[92] The Universal Declaration of Human Rights commences by stating that "*all human beings are born free and equal in dignity and rights.*"[93] Protocol No. 13 to the ECHR which intends to abolish death penalty in all circumstances noted that it was essential to abolish this practice in light of the fundamental right to life and *inherent dignity* of all human beings.[94] Waldron argues that dignity is a slippery notion.[95] Valentini notes that human rights are often understood as entitlements that all human beings possess by virtue of their 'inherent dignity' and that exist independently of legal or social recognition.[96] Renowned scholar Khaitan has noted that 'dignity' encompasses the value of 'respect' and 'reputation' of an individual.[97] This lays down a basic premise of what dignity essentially is and would be relevant within this section.

Dr. D.Y. Chandrachud J. in his opinion in the landmark *Puttaswamy* (Nine-Judge Constitution Bench)[98] decision by the Supreme Court of India had

[91] *Korematsu v. U.S.*, 323 U.S. 214 (1944) (Federal Supreme Court of the United States).

[92] *See* Pritam Baruah, *Human Dignity in Adjudication: The Limits of Placeholding and Essential Contestability Accounts*, 27 Can. J.L. & Juris. 329-356 (2014); Marcus Düwell, Jens Braarvig, Roger Brownsword & Dietmar Mieth (eds.), The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives, Cambridge University Press (2014); Carter Snead, *Human dignity in US law* in The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives 386–393, Cambridge University Press (2014).

[93] Universal Declaration of Human Rights, December 10, 1948, art 1 (UN General Assembly).

[94] Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms, concerning the abolition of the death penalty in all circumstances, May 5, 2002, ETS No.187 (Vilnius) (European Union).

[95] *See* Jeremy Waldron, Dignity Rank & Rights, Oxford University Press (2012); Jeremy Waldron, *Is Dignity the Foundation of Human Rights?* in Philosophical Foundations of Human Rights, Oxford University Press, 2015.

[96] Laura Valentini, *Dignity and Human Rights: A Reconceptualisation*, 37(4) Oxford Journal of Legal Studies 862 (2017).

[97] Tarunabh Khaitan, *Dignity as an Expressive Norm: Neither Vacuous Nor a Panacea*, 32(1) Oxford Journal of Legal Studies 4, 17 (2011).

[98] *See generally Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ^41 and 119 (*hereinafter* Puttaswamy) (Chandrachud, J. authored his opinion for Khehar, C.J., Agrawal, J. and Nazeer, J. It is important, however, to point out that Chandrachud, J. at ^298 states that privacy and dignity are also interdependent, noting that dignity cannot be exercised without privacy. This makes the argument for privacy being a facet of dignity as a *circular* and confusing argument. Bobde, J., has also supplemented the holding that 'privacy' and 'dignity' are interconnected at ^407 and ^411, albeit noting that privacy is necessary to exercise freedoms and rights guaranteed under Part III of the Indian Constitution (Chapter on Fundamental Rights). S.K. Kaul, J. at ^645 and 647 of the judgment, in his conclusion, had also agreed with the idea that 'privacy' and 'dignity' are

held that the evolution of the comparative framework of law and history (*including a 'right to privacy'*) reflects the basic need of every individual to live with 'dignity'. He noted that "*'dignity' is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence*."[99] Moreover, dignity has both an *intrinsic* and instrumental value.[100] We can therefore understand *privacy* to be a right contingent on the inalienable notion of *human dignity*. Going by this logic, were we to consider RTBF as a facet of 'privacy' or 'the control-based theories of privacy' (*as seen in the earlier sections*), RTBF should be automatically considered to be a sub-facet of *dignity*. However, we can also conceptualize RTBF as a directly derived facet of dignity.

Interestingly, a Single-Judge order rendered by Anand Byareddy, J. of the Karnataka High Court (India) in *Vasunathan*[101], had mentioned RTBF months before the landmark *Puttaswamy* decision recognized right to privacy as a fundamental right in India. Simply put, the facts of the writ-petition concerned reporting name of the petitioner's daughter in a judicial order on a criminal suit. While the petitioner's daughter had filed a criminal suit against her husband, she had later withdrawn it owing to a subsequent compromise. The order which acknowledged the compromise decree had mention of the petitioner's name and his daughter's name. It was contended before the High Court that if anyone were to do a name-wise search of the petitioner's daughter on an internet service provider (search-engine) like Google, Yahoo etc., the earlier judicial order would be likely to reflect in results of such a search by chance on the public domain. The reveal of this order could have repercussions that could extend to affecting the family relationships of the petitioner, as well as affect his daughter's reputation within the society. Therefore, the petitioner requested the court to direct the Karnataka High Court registry to 'mask' his daughter's name in the cause-tile of the order passed in the petition filed by her husband. Moreover, the petitioner also requested the court to direct the registry to take steps to mask the identity of his daughter, if her name is reflected anywhere in the body of the order apart from the cause-title, before the judicial order is released for the benefit of any service provider.[102] The court permitted the prayers of the petitioner, with a modification to not affect the display of the order as it is on the High Court website and any certified orders of the earlier High Court

---

intertwined. At ^609, Kaul J. had also observed that 'privacy' is a form of 'dignity', which suffers from the same inconsistency (i.e. circular argumentation) highlighted above for the judgment by Chandrachud, J.).

[99] *See id.*, ^119 (Chandrachud, J.).

[100] *See id.*, ^298 (Chandrachud, J.).

[101] *See Vasunathan v. Registrar General*, 2017 SCC OnLine Kar 424, ^1-5 (*hereinafter* Vasunathan).

[102] *See id.*, ^1-6.

order. The court further noted that it should be the endeavour of the registry to ensure that any internet search made in the public domain ought not to reflect the woman's name in the cause-title or body of the order, owing to the sensitivity of the cases involving woman in general, as well as highly-sensitive cases involving rape or affecting the modesty and reputation of the person concerned. The court recorded that this would be in line with the recent trend in western countries where RTBF is followed as a matter of rule.[103] Notably, the court never used the value of privacy in this order while referring to the RTBF.

There are various similarities between the ECJ's *Google Spain* decision and the Karnataka High Court's *Vasunathan* order. Before we delve into these similarities, it would be important to note a fundamental difference between *Google Spain* and *Vasunathan*. While the *locus standi* of the former case arose from Directive 95/46 of the EU under EU Law, the latter case was based on enforcement of fundamental rights, which were impliedly permitted by the High Court without any reference to a specific fundamental right under the Indian Constitution. *First*, the request for an order to direct search-operators/search-engines including Google, to remove name of a citizen from their websites or search-results pertaining to a judicial decision/order was made in both the cases. *Second*, the search-engines putting up the name of a citizen on their website in accordance with a judgment (in *Google Spain*) or in order to later display a judicial order by a High Court (in *Vasunathan*) on their search results, did so in accordance with law. *Third*, both the judicial decisions have invoked fundamental rights or constitutional values while allowing the restrain on search-operators to proceed.

As noted earlier, in *Google Spain* decision, the ECJ held that personal data of an individual concerns multiple facets of an individual's private life and therefore, the display of such an individual's name on the search results would violate their fundamental right to *privacy*. While privacy is constantly evoked by the ECJ in *Google Spain*, it is important to consider that the various facets of an individual's life that are recorded in their personal data can also be protected by the value of *dignity*. Notably, the use of expression "fundamental rights and freedoms, including the fundamental right to privacy" by the ECJ, as well as the EU's Directive 95/46 indicates that *dignity* is impliedly included to be one of the rights and freedoms that has the potential to be violated by the actions of the search-engines. Moreover, after Protocol No. 13 was added to the ECHR, it was recognized that all human beings have an 'inherent dignity' which would be a part of the guarantees under the ECHR. For the time-being, let us set aside the earlier

[103] *See id*., ^6-9.

understanding of *privacy* being interlinked to, or encompassed by the value of *dignity* acting as a larger supercluster of rights by judicial bodies such as the Supreme Court of India.

In *Vasunathan*, the Karnataka High Court emphasized on the 'respect', 'reputation' and 'modesty' of a woman while granting an order similar in nature to exercise of RTBF against search-engines. These are values which unarguably, *inter alia*, comprise the 'dignity' of an individual. *Additionally*, there was no reference to the value of *privacy* in *Vasunathan*. Hence, through the *Google Spain* decision and the *Vasunathan* writ order, one could argue that *dignity* has been impliedly used by the courts to direct search-engines to remove personal data (including name) of an individual from their search results. This indicates that RTBF could be argued to be a directly derived facet of *dignity* without any reference to privacy.

There are additional reasons to support the theoretical argument that RTBF is a facet of 'dignity'. Mali believes that the theoretical basis for a RTBF is based on the argument that a historical event related to an individual should no longer be revitalized due to the length of time elapsed since its occurrence.[104] Interestingly, the ECJ in *Google Spain* did seem to take into account the time elapsed since the case against the complainant in Spain for recovery of debts had been completed, while deciding whether the complainant's rights under Directive 95/46 are being violated.[105] This indicates that after a *passage of time*, the 'respect' or 'reputation' attached to the personal data about an individual's life can be considered to be harmed, if not for exercise of a restrain on search-operators. Moreover, the ECJ noted that 'inaccuracy of data' or 'not keeping data up-to-date' can also be considered to be situations warranting a data-subject's right to object.[106] Inaccuracy of data would simply mean that the personal data on an individual is misrepresentation of their life and its surrounding facets. This could clearly envisage situations where the respect or reputation of an individual could be affected, leading to a violation of their *dignity*. Similar would be the case where personal data displayed on an individual is not kept up-to-date. Consider a simple example where an appeal is being heard against conviction of an accused and on appeal, the subordinate judicial authority's decision is overturned. In such case, the accused shall be no longer treated as a convict and would be legally entitled to have been respectfully absolved of the charges. In this case, any data which is not up-to-date shall be misrepresenting the status of the individual who has been absolved of all charges and would interfere with their respect or reputation

[104] *See* Mali, *supra* note 12, 7.
[105] *See* Google Spain, *supra* note 11, ^62.
[106] Id.

in the society. This would be another situation warranting invocation of the RTBF to erase the not up-to-date data.

In light of the above analysis, I would light to conclude this section by noting that RTBF can indeed be jurisprudentially considered to be a facet of dignity, whether indirectly (as being a facet of *privacy*, which is in turn a derived facet of *dignity*) or directly as a facet of dignity.

4. Theoretical Indeterminacy: Is RTBF a misappropriation of the existing protections envisaged under the 'right to privacy' jurisprudence?

As mentioned previously, not only have scholars remarked that right to privacy protects *personal data*, even the EU Law and general principles of community law (reflected in the Directive 95/46) itself acknowledge this fact. Data privacy or Informational Privacy (i.e. privacy vis-à-vis personal data) has been subject to academic discussion for decades.[107] Recalling Khamroi and Shrivastava's argument, it is apparent that other rights or values such as liberty, autonomy and dignity provide agency to an individual in performing certain private acts, without any "external interference".[108] Unlike privacy, these rights/constitutional values do not reflect the psychological aspects of the act committed by a person.

Privacy performs an important role in allowing an individual to shape their 'personality' or 'identity' in a manner they desire, which is a necessary pre-condition to the performance of a private act without any "internal reservation". Privacy addresses the concerns regarding "internal reservations" by protecting "*all information/data integral and incidental to the private acts of a person, which are done in exercise of their liberty or autonomy.*"[109] In light of the foregoing understanding, Khamroi and Shrivastava have lucidly defined privacy as the "*right to prevent others from wrongfully or illegally accessing and/or misappropriating personal information, notwithstanding the public availability of such information.*"[110]

[107] Daniel J. Solove and Paul M. Schwartz, *An Overview of Privacy Law* in Privacy Law Fundamentals, IAPP (2015); Christina P. Moniodis, *Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy*, 15(1) Yale Journal of Law and Technology (2012); Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies, 6-7, 94, Harvard University Press (2018); Ingham, *supra* note 4; W.A. Parent, *supra* note 4; Khamroi and Shrivastava, *supra* note 4, 106.
[108] *See* Khamroi and Shrivastava, *supra* note 4, 105.
[109] For a greater understanding about the concept of "internal reservations" and its difference from "external reservations", *see id.*,105-106.
[110] *See id.*, 106.

This definition of privacy is similar to the scope of RTBF that we saw earlier in Part 3.1.[111]

Let's now recall the earlier observation on how personal data/information is being protected by two rights, i.e. right to privacy and RTBF.[112] Evidently, both the RTBF and right to privacy are protecting the *personal data* of individuals/data-subjects, notwithstanding its public availability from wrongful acts, non-consensual or illegal access and potential misappropriation. In light of the already well-established jurisprudence on *privacy*, there would be no need for *privacy* as a separate RTBF. Vice-versa, if *RTBF* is accepted the way it is in the EU jurisprudence, there would be no need for privacy, as other rights or values such as RTBF, liberty, autonomy, dignity are capable of covering individuals from both external interferences and internal reservations. While one could argue in favour of RTBF and say that privacy is a "bundle of rights" which covers various forms of actions in public and private spaces, the fact that rights/values other than RTBF cover such actions would mean that privacy is in fact redundant. This shows us that the co-existence of both right to privacy and RTBF leads us to a state of *theoretical indeterminacy*, where we cannot outline the scope of one right over another, unless we treat both the rights as essentially the same rights, or eliminate one of them on ground of redundancy.

However, the jurisprudence on right to privacy emerged way back in the 19th century era, with one of the earliest writings being those by Warren and Brandeis (where they called 'privacy' as a human right)[113] and Cooley (who coined the phrase "right to be let alone")[114], both of whose works have been closely associated with privacy. Moreover, RTBF/RTE in the EU jurisprudence itself stems from the existing fundamental rights and freedoms under EU Law, *in particular*, the right to *privacy*. This right to *privacy* is derived from the ECHR and the general principles of EU Law, as recorded by the ECJ in the *Google Spain* decision. Further, the table provided below shows nine provisions or recitals from Directive 95/46

[111] *See* discussion *supra* Part 3.1.
[112] *See* discussion *supra* Part 3.2.
[113] *See* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 205 (1890). Importantly, several scholars have highlighted the work of Warren and Brandeis as being one of the most impactful legal articles and the most important scholarship on privacy, *see* Harry Kalven, Jr., *Privacy in Tort Law – Were Warren & Brandeis Wrong?*, 31 Law & Contemp. Probs. 326, 327 (1966); Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech,* 63:5 Vanderbilt Law Review 1296 (2010). In his article, Richards also considers Justice Brandeis to be one of the most influential figures to have influenced the development of global privacy jurisprudence, especially through his legacy as an Associate Justice of the Federal Supreme Court of the United States of America and as a scholar/academic.
[114] *See* Thomas M. Cooley, Law Of Torts 29 (1880).

(which preceded the GDPR), that have an express or implied reference to *privacy*, while governing aspects related to *personal data* [refer to Table A below].

TABLE A:
Provisions or Recitals in Directive 95/46 of the European Union which expressly or impliedly refer to 'privacy' or 'right to privacy'
[Source: Directive 95/46.]

S. No.	Recital/Article	Relevant extract from the text [emphasis added]	Express Reference	Implied/ Indirect Reference
1.	**Recital 2**	"*their fundamental rights and freedoms, notably the right to privacy*"	Yes	No
2.	**Recital 10**	"*... notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms... and in the general principles of community law*"	Yes	No
3.	**Recital 18**	"*... in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive,... in accordance with the law of one of the Member States...*"	No	Yes
4.	**Recital 19** **Note**: As EU Law is	"*... that each of the establishments fulfils the obligations imposed by the national law*	No	Yes

	transposed into EU member states, right to privacy would automatically become a part of the internal/national law of the EU Member State.	*applicable to its activites*"		
5.	**Recital 20**	"*... the protection of individuals provided for in this Directive... ensure that the rights and obligations provided for in this Directive are respected in practice;*"	No	Yes
6.	**Recital 25**	"*... the principles of protection must be reflected,... and, on the other hand, in the right conferred on individuals...*"	No	Yes
7.	**Article 7(f)**	"*interests [or] fundamental rights and freedoms of data subject...*"	No	Yes
8.	**Article 9**	"*...right to privacy with the rules governing freedom of expression*"	Yes	No
9.	**Article 28(4)**	"*... the protection of his rights and freedoms in regard to the processing of personal data*"	No	Yes

Both the discussions throughout this article and the empirical observations from the above-mentioned data (with nine express or implied references to

privacy), it is sought to be demonstrated that RTBF/RTE is not a new right created by the *Google Spain* decision or the GDPR, but it is a facet of *privacy* or rather 'right to privacy' itself. It is here that a challenge comes to the jurisprudence and scholarship on RTBF in the EU, which forwards the idea of RTBF as a new, separate and distinct right. Moreover, a greater difficulty which would be faced by proponents of RTBF in distinguishing it from privacy would be to exactly lay down what constitutes the nature of RTBF, which is not already covered and protected by privacy. This shows us that it is extremely difficult or potentially impossible to lay down the exact scope and nature of RTBF, while distinguishing it from privacy. Consequently, one can conclude that RTBF is an attempt by the EU Parliament or drafters of the GDPR to portray creation of a new right which protects "personal data", which is actually *privacy* or a derived form of applied *privacy*, in garb of a new right. This is supported by the fact that there is not a single mention of the term 'privacy' in the GDPR's text. The fact that it is difficult to conceptualize RTBF/RTE as an independent right which protects 'personal data', as well as its coexistence with a right to privacy that also protects personal data are the two major jurisprudential fallacies of the RTBF jurisprudence. Thus, I conclude this segment by arguing that RTBF is privacy itself, or alternatively, a derivate of privacy.

5. Practical Limitations of RTBF/RTE and Balancing 'Competing Interests'

Through this article, we have understood the origins of RTBF/RTE in the EU. We have also ventured into jurisprudential/theoretical analysis of whether RTBF is an independent right or a derived right, as well as discussed the problem of theoretical indeterminacy created by co-existence of RTBF with the already existing and well-established right to privacy.

In this segment, I shall now discuss certain practical limitations of RTBF with illustrations. These discussions will also invoke the concept of "balancing". However, the reference to comparative jurisprudence in this segment shall be very limited or avoided, in order to best attempt to evade the fallacy of academic engagement in the form of "generic constitutional law" as described by Hirschl.[115]

[115] *See* Hirschl, *supra* note 72, 12. While I do acknowledge Hirschl's criticism of academics/writers erroneously making a universalization of constitutional law and jurisprudence (while writing using a style of comparative constitutional law or comparative writing) as valid, I do not find Hirschl's argument as perfect and believe that it is open to challenge.

5.1. Commercial Surveillance and Commercial Interests

The ECJ in *Google Spain* had categorically observed that the provisions of Directive 95/46 permit 'legitimate interests' as a valid purpose for which, a controller, or third party, or parties to whom the data is disclosed can *process* personal data. It also cautioned that generally the interests of fundamental rights and freedoms, including right to privacy, of the data subject with respect to the processing of personal data that requires protection under Directive 95/46 would override the competing legitimate interests of the other parties (such as controller/third party).[116] Moreover, it added that a 'balancing' of the opposing rights and interests of the data subject and other parties need to be taken into account by a legal authority, while remembering the significance of the data subject's rights arising from Article 7 and Article 8 of the ECHR.[117] The ECJ recorded that due to potential seriousness of the interference caused to a data subject's rights by a controller's actions, merely the 'economic interest' of the other party wouldn't be sufficient to justify a legitimate interest.[118]

At the same juncture, while a data subject's right generally overrides the legitimate interests of any internet users who would be potentially interested in having access to the personal data of the data subject, a balancing of the competing interests would "*depend on the nature of the information in question and its sensitivity for the data subject's private life*."[119] Further, the 'interest' of the *general public* in having access to that personal data (the interest being variable depending on the role played by the data subject in public life) must also be taken into account.[120] In addition, the *publisher* of a web-page which consists of personal data relating to a data subject could in *some circumstances* carry out the processing, solely for *journalistic purposes*. The foregoing publication of a web-page would be permissible by virtue of benefits available to the publisher provided by the derogations envisaged in Article 9 of the erstwhile Directive 95/46[121] (which is currently governed by modifications brought by the GDPR). The legitimate interests assigned to the activity of search engines may differ than those assigned to a publisher working solely for journalistic purposes, which may have different impact on a data subject's personal life. To illustrate this, the ECJ recorded that in certain circumstances, the RTBF of the data subject would be exercisable only against an operator, but not publisher of a web-page. Recalling our discussion in Part 2.2, the request by complainant to direct the

[116] *See* Google Spain, *supra* note 11, ^62, 96.
[117] *See id.*, ^62.
[118] *See id.,* ^81.
[119] Id.
[120] Id.
[121] *See id.,* ^85.

newspaper publisher to remove the publication was rejected by the Spanish Authority (AEPD) on the ground that the *processing* done by the news publisher and the web-operator (i.e. Google Spain) were done pursuant to different purposes/legitimate interests. The purpose of the processing by the news publisher was to lawfully report a judicial decision solely for journalistic purpose and no other commercial interest.[122]

As discussed previously in Part 3.1, the ECJ held that while appraising requests for RTBF, judicial authorities or other competent authorities must examine whether the data subject has a right, *at this point in time*, that information relating to them personally, "*should no longer be linked to their name by a list of results displayed following a search made on the basis of their name.*"[123] To simplify, a judicial authority/competent authority would have to examine whether: *first*, a data subject has a right to object to the lawful display or sharing of their personal data by a controller [a.], and *second*, whether the passage of time justifies the foregoing right to object [b.].

A collective reading of the above-mentioned discussion would reveal a test for *balancing* the interests of 'commercial entities' or 'other' parties/persons and the 'data subject' collectively, by a judicial/competent authority in the EU, for cases involving an invocation of the RTBF. The test is simplified as follows (in consecutive step-by step manner):

1. A determination must be made as to whether the 'data subject' has a *right to invoke RTBF* against processing of personal data. The *passage of time* should justify the data subject's right to object, which is entirely a discretion[124] for the judicial/competent authorities, unless the member state's law expressly lays down a standard for determining this passage of time.
2. The entity lawfully processing the personal data (*whether a controller, publisher, third party, party to whom personal data is disclosed etc.*) must have legitimate interests for processing which must not merely be limited to economic interests. It is essential to demonstrate the 'necessity' of these legitimate interests. Although if processing is only for *journalistic purposes*, it may suffice as a legitimate interest.
3. The *nature* of the information in question and its *sensitivity* for the data subject's private life must be taken into account. It is important to

[122] *See* discussion *supra* Part 2.2.
[123] *See* Google Spain, *supra* note 11, ^96.
[124] Notably, the Google Spain case did not expressly lay down any guidelines to determine whether there has been a justifiable lapse of time or passage of time to exercise the 'right to be forgotten'. However, the ECJ considered a period of 16 years to be a reasonable time for the data subject to invoke the foregoing right, *see* id., ^98.

ascertain how the nature and sensitivity of the information impacts the *interest of the general public* in having this information.

4. The *consequences* of processing of the personal data on a data subject's rights must be taken into account. Different entities may have varying justifications for processing.
5. A balancing of the competing interests of a person or commercial entity processing the data and the data subject's rights must be done. As a general rule, the data subject's rights are placed at a higher pedestal than the legitimate interests of the commercial entities or other persons/parties.

If we follow the above-mentioned five-step test, we can *balance* the *commercial interests* of commercial entities/other parties against a data subject's *RTBF*. A fallacy, however, of the above test is that it does not consider whether the data subject had actually *consented* to provide the personal data or not. Nonetheless, a judicial/competent authority can consider the element of 'informed consent' at the final balancing stage.

Let us now consider the following three illustrations (apart from the legitimate interest of 'journalistic purposes' discussed earlier) in order to consider practically balancing a RTBF in light of *commercial surveillance* in the digital age of internet:

Illustration I: Consider that an individual is using a social-media platform like Facebook, Instagram or LinkedIn. While using these platforms, there are third-party apps or pages that would permit the individual to utilize the apps or access the page, provided the data subject consents to share this data with the third-parties. This allows third-parties to do commercial surveillance based on your personal data, which potentially includes your personal interests or followings. Here, the interests of both the data subject, social-medial platform and third-party apps would be automatically balanced so far, since the data subject *consented* to providing the data to the social-media platform, and subsequently, to the third-parties. However, on the passage/elapsing of time, a data subject would still retain the right to seek erasure of the personal data which would have to be re-examined by a competent authority.

Illustration II: Consider that you're using a social-media platform to connect with your friends. You utilize an inbuilt application on this platform which is owned by a commercial entity or registered company. This app requires you to complete surveys on thousands of matters, but informing you that the collection of this information is only for academic purposes. The platforms design (which may be either an intentional design or with lacunae in security) allows the app to not only collect survey details from

you, but also to provide all personal data on your profile to the third-party app. Moreover, anyone who's in your social network as a friend has their personal data collected by the same app owing to inherent design of this platform due to your use of the app. This personal data collected by the third-party app without the consent of the platform user or their social-network friends is ultimately utilized for commercial purposes such as targeted commercial surveillance on the platform users or for political purposes by commercially trading information with politicians or political entities. This example is based on the *Cambridge Analytica-Facebook* controversy as reported by The Guardian.[125] In such a situation, permitting a commercial surveillance would severely impair the rights of a 'data subject'. While the *Cambridge Analytica-Facebook* controversy was based on acquiring personal data through illegal means, there can be situations where even if the app takes the personal data of the users with their consent, the transmission of this information can lead to manifestly severe consequences on the rights and life of a data subject, including leaks of political preferences, ideologies, religion, gender etc., which can make the data subject a target for political groups. In such a situation, the overwhelming rights of a data subject would override any legitimate interests of other parties, even if the data subject's consent is taken expressly for commercial purposes, as passing on of such data can pose a risk to the data subject's life.

Illustration III: Every internet browser that we use in daily life such as Mozilla Firefox or Google Chrome, relies on collection of data called as "cookies" which keeps a track of our activity, the websites we visit, the materials we download or access and potentially store our personal data obtained by generally navigating using an internet browser. The default setting of each of these internet browsers is to collect and download cookies from every web link we successfully access. This data is collected and stored on our computers or mobile phones or tablets, occasionally being duplicated in cloud-storages. There are often websites that use data from these cookies stored by the browsers with or without our consent (subject to

125 For understanding the Cambridge Anlaytica-Facebook controversy, kindly sequentially refer to the following news articles by The Guardian, *see* Ted Cruz, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, The Guardian, December 22, 2015, available at: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data (Last Visited on May 25, 2021); Carole Cadwalladr, *The great British Brexit robbery: how our democracy was hijacked*, The Guardian, May 7, 2017, available at: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (Last Visited on May 25, 2021); Carole Cadwalladr and Lee Glendinning, *Exposing Cambridge Analytica: 'It's been exhausting, exhilarating, and slightly terrifying'*, The Guardian, September 29, 2018, available at: https://www.theguardian.com/ membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie (Last Visited on May 25, 2021).

utilization of a strict anti-cookie use settings of our browser). Using our IP address, they can track our location (unless one uses a perfect VPN or proxy). This information collected by the websites cannot be traced by the user and can be effortlessly shared by the websites with third-parties or others interested in user data to perform commercial surveillance. In certain situations, these websites can do commercial surveillance by themselves for internal or external uses. A user could start seeing targeted advertisements on the internet based on the user's data available in the cookies, like suggestions to buy a Bugatti, Ferrari or McLaren vehicle, to buy shoes from Adidas or Nike, or even book hotels or flights, which are common in the modern age of internet. In such a situation, the only significant interest of the websites would be to acquire personal data for their own economic interests. This circumstance would by itself not justify being a necessary 'legitimate interest', and would strongly warrant a balancing in favour of the overwhelming rights of the data subject over their personal data.

5.2. State Surveillance and Public Interest

Before commencing a discussion on *state surveillance*, it would be important to point out that the same five-step test elaborated in the previous sub-segment [Part 5.1] would apply to a *controller* who is a part of the EU member state or is processing personal data on the directions of the state. However, there are certain changes to the weight given to *public interests* or *legitimate state interests*, while balancing these interests against a data subject's RTBF.

The ECJ in *Google Spain* recorded that a EU member state is permitted to lay down legislative rules or guidelines in its internal laws to permit processing of an individual's personal data for *historical, statistical* and *scientific purposes* under the erstwhile Directive 95/46. This can be done even where the personal data is stored or caused to be stored for a *very long or indefinite amount of time*.[126] As noted earlier, the GDPR still enables the foregoing purposes to stand as exceptions, which permit the processing of an individual's personal data.[127] These are all grounds which inarguably form a part of the *general public interests* or *legitimate state interests*, which enable processing of the personal data by a controller.

The ECJ also acknowledged that internet users would have a *legitimate interest* to an individual/data subject's personal data due to simply being interested in having access to that information. This interest of internet users would have to be balanced with a data subject's rights, while considering

[126] *See* Google Spain, *supra* note 11, ^94.
[127] *See* discussion *supra* Part 2.3.

the 'nature' of information in question and 'sensitivity' for the data subject's private life.[128] Moreover, the ECJ recorded that while determining whether the data subject's rights (including the RTBF) under the EU Law are exercisable, the legitimate interest of the *general public* in finding that information upon a search relating to the data subject's name must be considered. The interference with fundamental rights of a data subject could be justified by the *preponderant interest* of the general public in having access to the personal data (information) in question.[129] However, unless the role played by the data subject in *public life* makes an interference with their rights justified by this preponderant interest of the general public by accessing the data subject's personal data, the rights of the data subject would override even the interest of the general public.[130]

Consequently, in order for a state to justify intrusion into an individual's rights (including the exercise of the RTBF by a data subject over their personal data), it has to justify the existence of a preponderant interest of the general public in accessing the personal data of the data subject, owing to the role played by the data subject in "public life". Moreover, in order to collect the personal data of the data subject for historical, statistical or scientific purposes, it has to create legislative guidelines or rules which are assumed to follow the principles of proportionality. Here, the phrase "public life" is *vague* (unless expounded on by a legislation) and would have to be interpreted by a competent authority on a case-to-case basis, while balancing the competing legitimate interests of the state and the individual's rights over their personal data.

Let us now discuss how the above-mentioned standard for justifying a state's interest or public interest into interfering with a data subject's RTBF would play out with the following illustrations:

Illustration I [Targeted Mass Surveillance]: Interestingly, the inclusion of the exception of 'statistical purposes' would allow an EU Member State to conduct *mass state surveillance* on the grounds of *preponderant public interest* for any legitimate cause deemed necessary by the state. A state could easily create a law which encroaches or intrudes into an individual's rights, while incorporating the principles of proportionality and satisfying the requirement of the existence of a valid law. Ultimately, whether such a mass surveillance measure is proportionate or not depends on the competent/judicial authorities in that member state. This would include schemes similar to that of a census of citizens and residents, or identification

[128] *See* Google Spain, *supra* note 11, ^81.
[129] *See id.,* ^97.
[130] *See id.,* ^99.

of an individual aimed at targeted delivery or distribution of goods and services such as *Aadhaar* in India[131], and any other schemes which intend to identify public and categorize them on the basis of an individual's personal data to provide them protections or guarantees (such as a simple natural disaster relief mechanism targeted at identifying people living in dangerous or hazardous areas and guiding them to safety). At the same juncture, some states could also modify and use 'personal data' of individuals to identify and target minority religious or cultural or foreign or gendered communities within their sovereign territories. While it is likely that the ECJ or judicial authorities will consider such a scenario as outright impermissible under the GDPR, the ground of 'public interest' in such situations could become a dangerous tool for competent authorities (including judicial authorities) in a EU member state to justify balancing of the state's legitimate public interests and an individual's personal data, which could include their religion, gender, sexuality, culture, race etc.

Illustration II [Public Offices or Statutory/Constitutional obligation to disclose personal data to the public over certain positions]: Most states in the world put the name of all the public authorities and their officials on display in their documents, websites and official gazettes etc. Generally, not only the name and positions of the public authorities are disclosed, but so is their personal information including their education, department, expertise, age, retirement etc. This could serve as personal data of an individual which is in the preponderant interest of the general public to be known and be easily accessible. Such an intrusion can be justified by the state on grounds of legitimate public interest. Similarly, the internal laws of a member state may often mandate corporate/company-related individuals (such as those who are directors, chairpersons, shareholders of a company or attached to a company in a similar fiduciary capacity) to disclose their position to the public. This is often done by making the articles of association, memorandum of association or shareholders agreement of a company etc., available to the general public in public domain. Such cases are often justified due to the common law doctrine of *constructive notice*[132] which states that the foregoing documents which are statutorily mandated to be in public domain are considered to be known to an individual (or rather the

[131] Suhrith Parthasarthy, *Aadhaar: Enabling a form of supersurveillance*, The Hindu, January 16, 2018, available at: https://www.thehindu.com/opinion/lead/aadhaar-enabling-a-form-of-supersurveillance/article22444686.ece (Last Visited on May 25, 2021); Kathryn Henne, *Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India* in Information, Technology and Control in a Changing World 223-45, Springer (2019).

[132] *See Oakbank Oil Co. v. Crum*, 1882 8 A.C.65 (House of Lords, United Kingdom). This UK House of Lords decision is considered to be the oldest authority on 'doctrine of constructive notice' in common law.

general public) who may contract with or deal with a company for any lawful purposes. Under common law, it is considered that the general public has a right to know the basic information about a company owing to commercial or contractual necessities, as well as the impact of companies on a state's economy. This would simply mean that the role of a company (as well as its officials) in its public life is considered to be of *public nature* and not sensitive enough to be protected from public scrutiny.

Illustration III [Celebrities]: As discussed previously in this sub-segment, the ECJ observed that while balancing the preponderant general interests of the public to acquire personal data of an individual, it is important to consider what role is played by the individual in their *public life*. Individuals such as actors and others in the cinema industry, sportsperson, Olympics participants, as well as other individuals comprise what we know generally as "celebrities". These celebrities earn their reputation or brand by the virtue of their work or position in the society, which is in the realm of their public life. However, unlike the personal data of public officials in the preceding illustration, it is subjective as to what nature of information could be disclosed about celebrities and to what extent would personal data of celebrities relating to their life can be sensitive in nature. A simple way to dissect this would be to address the public-private divide in an individual's life. With regard to a celebrity, it would be important for a judicial authority to examine whether the personal data concerning a celebrity is something that falls within the category of private data (or data which must be protected from public domain) or whether it comprises an element of a celebrity's public life which could have an impact on the society or any industries. There is often a possibility of hard-cases where it is difficult to distinguish between what is 'private' information and what should be treated as 'public information'. Solutions to the circumstances concerning exercise of a RTBF by a celebrity would be to lay down legislative guidelines distinguishing private information from public information, or to permit the competent authorities (including judicial authorities) to subjectively determine what constitutes personal data in the public nature. If personal data falls within something that is in the public nature, it could be justified as being in the preponderant interest of the general public to be known publicly.

5.3. Chilling Effects

While RTBF plays an important role in protecting an individual's personal data, the exercise of this right has the potential to create 'chilling effects' on another individual or organization's competing fundamental rights and freedoms, especially the right to freedom of speech (including freedom to

express academic writings or speak about information in discussions), right to information and the freedom of press.

Murthy defines *chilling effect* to occur "*when an act inhibits the full utilization of the freedom of speech*."[133] The European Court of Human Rights (*hereinafter* **ECHR Court**) in *Goodwin v. UK* had to adjudicate a case, where a journalist was ordered by authorities in the UK to disclose the source of information disseminated by him in public domain. [134] Recognizing that "*the protection of journalistic sources was one of the basic conditions of press freedom*", it underlined the role of media as a public-watchdog. The ECHR Court acknowledged the importance of free flow of information, as well as the *chilling effect* on speech and the self-censorship that emanates from a lack of journalistic privilege.[135] Similarly, the Supreme Court of India in the *S. Khushboo* decision had made an important observation on 'chilling effects', recording that criminal cases filed against an individual/author for mere expression of thoughts curb their right to freedom of speech and expression, thus creating *chilling effects* on their rights.[136]

Scholars such as Lubis have made a scathing criticism of the *Google Spain* decision by the ECJ, terming the 'RTBF' as equivalent to a 'right to censorship' used against individuals.[137] Divan has argued that the combined reading of the Directive 95/46 and the *Google Spain* decision is problematic since the EU law authorizes private entities like Google or Yahoo to determine whether or not *personal data* related to an individual available in

[133] *See* L. Gopika Murthy, *Journalistic Privilege: The Vacuum in India*, 3 NLUD Student Law Journal 19 (2015).
[134] *See Goodwin v. United Kingdom*, App. No. 17488/90, 22 Eur. H.R. Rep. 123 (1996), ^39.
[135] Id.
[136] *See generally* S. *Khushboo v. Kanniammal and Anr*., (2010) 5 SCC 600, ^45, 47, 50 (The case concerned various criminal suits brought against the appellant who had made a remark on marital sex in the public domain. Here, utilizing the proportionality approach, the court held that if the competent authorities start imposing criminal cases on situations not warranting an intrusion on right to freedom of speech and expression, then it would lead to a 'chilling effect' on the foregoing right of an individual. The court observed that dissemination of news (with subjective opinions) for popular consumption would be permissible under the constitutional scheme of India. Moreover, an expression of opinion in favour of non-dogmatic and non-conventional morality has to be tolerated as it cannot be a ground to penalize an author.).
[137] *See* Tika Lubis, *The Ruling of Google Spain Case: 'The Right to Be Forgotten' or 'The Right to Censorship'?*, Social Science Research Network (SSRN), November 25, 2015, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2872874 (Last Visited on May 25, 2021) (*hereinafter* Lubis).

the public domain is violative of the data subject's right.[138] She further points out that there's a *potential* of *chilling effect* on free speech, since authorizing private entities may indulge in 'overregulation' in order to avoid litigations or claims for damages by removing web-pages or search results showing the name and personal data of a data subject, rather than objectively determine whether or not a data subject's RTBF has been violated.[139] A litigation suit or claim for damages can lead to heavy costs being imposed on the private entities or non-state operators owing to both the length of the litigation suit or having an order obtained against them, even while their display of information is lawful in nature. In order to appeal an adverse order, such a private entity or non-state operator would have to again engage a lawyer or legal team, which will cost additional money and time while the outcome of a successful appeal would be uncertain. Therefore, overregulation would be a money-saving and time-saving method to avoid any claim for damages or other litigations for a private entity or an operator.

Importantly, Lubis has shown how articles related to discrimination, stigmatization, racism, rapes/sexual-assault and other crimes were taken down from Google's search results on the grounds that they were inadequate, excessive, irrelevant or no longer relevant.[140] This, Lubis argues, demonstrates an excessive form of intrusion or censorship into freedom of press and the right to information of individuals. In effect, we can also see this use of RTBF as akin to its conceptualization as a facet of 'autonomy' or 'control-based' theories of privacy, which provide individuals a near-absolute control over their personal data, including a near-absolute and excessive use of RTBF.[141] Under the public interest limitations that we discussed in the previous sub-segment [Part 5.2], freedom of press and right to information of individuals can be justified by the state as a preponderant legitimate interest necessary for disclosure of personal data. However, the fact that the controller/operator (private entities like Google/Yahoo) have the first opportunity and full discretion in deciding whether to remove publicly available personal data of a data subject who's exercising a RTBF, makes it difficult to counter censorship by the controller, considering their overregulation tendencies.

Let us consider a situation where a person has been lawfully convicted by a court of law in an EU member state for grave offences such as murder, culpable homicide, rape/sexual assault, battery etc. As per the reformative

[138] *See* Madhavi G. Divan, *How Free Is Speech In The Age Of Social Media?*, 2 SCC J-13 1-18 (2017) (*hereinafter* Divan).
[139] Id.
[140] Lubis, *supra* note 137.
[141] *See* discussion *supra* Part 3.3.

theory of justice, such individuals have a potential to reform and be reintroduced in society. However, following the retributive theory of justice, such individuals have the potential to be a threat in future to other individuals in the society. This is the precise reason why laws in nation states may mandate a convicted criminal to be registered as a sex-offender or a murderer/killer. Such criminal convictions and registrations often have other legal consequences on an individual's rights and employment under the internal laws of a state. In such a situation where there's a potential of threat from individuals with conviction for grave offences and the conviction sentence has been announced by a court of law (i.e. a public forum and publicly available to the world), one should not allow censorship of media reports or of the common public discussing conviction of these individuals in public or private spaces using the RTBF, especially on the ground that there has been a *passage of time*. If RTBF is allowed to prevail here, then not only would the right to information and right to freedom of speech and expression of the general public be censored and suffer from a chilling effect, a state's legitimate interest in letting its public know about an individual's grave criminal record would be upset.

We must not *forget* (pun intended) that, the RTBF isn't an absolute right under the EU Law.[142] An individual/data subject cannot argue that they have a "right to not be known by others", i.e. a right to never appear in a search-engine's results in the first place. As per the GDPR, a data subject must discharge a burden before the competent authorities to demonstrate that their legitimate interest in having their *personal data* removed from online public forums/spaces has an overriding effect on the legitimate interests of the competing parties. If we permit the RTBF to be exercised in an unfettered manner and prevail over other fundamental rights and freedoms automatically, we would be walking into oblivion and a road to censorship.

6. Comparative Analysis: EU and India

Throughout this article, we have understood the origins, scope, jurisprudence and practical limitations of RTBF. In this segment, I shall be making a brief comparative analysis of the EU and India.

In India, there is a constitutional and legislative silence on both *right to privacy* and the RTBF. While there did exist a very restricted right to privacy through evolving case-law jurisprudence in India (some of which were contradictory)[143], the landmark *Puttaswamy* decision by a Nine-Judge Constitution Bench of the Supreme Court of India had *unanimously*

[142] *See* discussion *supra* Part 2, Part 3.1.
[143] ICLR, *supra* note 4, 1-18.

declared right to privacy as a fundamental right under various provisions of the Indian Constitution.[144] Before delving into the *Puttaswamy* decision, however, it is important to discuss some of the cases that came before Indian courts in the nature of seeking a RTBF.

In the *Dharmraj Dave* case, an individual had filed a petition before the Gujarat High Court, praying for a "*permanent restraint on free public exhibition of a judgment and order*" in which he was involved.[145] The earlier case involved criminal proceedings against the individual petitioner for a number of offences including culpable homicide amounting to murder, from which he was acquitted. The individual contended that in spite of the judgment in the previous case being designated as unreportable by the High Court, an online repository of judgments had published it, and consequently, it was also indexed by Google Search on its web-results. The request of the individual in the foregoing case was dismissed by the High Court on two grounds. *First*, the individual was unable to point out any provisions of law that assisted his plea. *Second*, it was held that a website publication does not classify as reporting, since reporting only pertains to the publication of the judgment by law reports. It is pertinent to note that while the prayer made by the individual was similar in nature to seeking an exercise of RTBF in EU Law, there was no express mention of RTBF or even the right to privacy.

On the other hand, as seen in the case of *Vasunathan*[146] [which was discussed earlier in Part 3.4], we saw how a Single-Bench of the Karnataka High Court comprising of Anand Byareddy, J., had allowed for an individual's plea to have his daughter's name removed from the earlier judgments/orders, present proceedings and cause-list of the cases (except where the publication was done on the High Court website or a certified copy of the judgments/orders was sought). The court also expressly recognized that the remedy sought by the individual on behalf of his daughter was similar to RTBF in the western jurisprudence and permitted the request. Unlike the typical RTBF cases in the EU, this case sought to exercise RTE of name/personal data against the registry of a High Court over *lawfully* given judgments. The court did not, however, refer to any constitutional provisions or earlier precedents on the limited right to privacy while granting remedy to the individual petitioner. Nonetheless, the court in this case exercised its inherent powers to grant plea of the petitioner, displaying a progressive approach and understanding about the importance of time and reputation/dignity of the individual. Notably the court also

[144] Puttaswamy, *supra* note 98.
[145] *Dharmraj Bhanushankar Dave v. State of Gujarat*, Special Civil Application No. 1854/2015 (High Court of Gujarat) (*hereinafter* 'Dharmraj').
[146] *See* Vasunathan, *supra* note 101, ^1-5.

recorded that any internet search made in the public domain ought not to reflect a woman's name in the cause-title or body of the order, owing to the sensitivity of the criminal cases involving woman in general, as well as "*highly-sensitive cases involving rape, affecting the modesty and reputation of the person concerned.*"[147] This is strongly reminiscent of the emphasis on sensitivity and personal life of a data subject in the EU. Given the fact that the *Vasunathan* decision was delivered before the *Puttaswamy* decision by the Supreme Court of India had declared right to privacy as a fundamental right, Byareddy, J.'s approach in this case is remarkable and highly commendable.

Another relevant case prior to the *Puttaswamy* decision, is *The Case Concerning Blue Whale Challenge*[148] which was before a Division-Bench of the Madras High Court. In this case, the High Court had an opportunity to discuss RTBF in the EU jurisprudence and apply it in context of the Indian jurisprudence, although it did not substantively do so. Owing to the facts of the case, a long discussion on RTBF was not necessary for the court, although it did substantively discuss the role of controllers/operators in the EU. In this interesting case, the court had taken *suo-motu* cognizance of the fact that a college student had committed suicide, while attempting the Russian trend of Blue Whale Challenge. The deceased student had left a powerful suicide note describing the Blue Whale Challenge and stated that once a person enters into this challenge, it is extremely difficult to escape it. The court recorded that this challenge involves a person to do over fifty difficult activities, the culmination of which leads into self-destruction or suicide. It further recorded that the trend had mostly targeted the younger individuals of the society. On this understanding, it observed that the EU jurisprudence on RTBF has shown how service providers (controllers) can be directed by judicial authorities to regulate their content. Moving forward, the court made the following remark:

> "*The service providers cannot abdicate their responsibilities. They cannot also plead that they have no control over the content. A mere look at the net neutrality debate that is presently going on would show that the service providers are in a position to have control over the content that passes through their information highway. If the service providers can attempt to control the content for commercial considerations, they can certainly be called upon to exercise their*

[147] Id.

[148] *See Madras High Court, The Registrar (Judicial) v. The Secretary To Government*, Suo Motu W.P. (MD) No. 16668/2017, ^1-22 (Madras High Court) (*hereinafter* The Case Concerning Blue Whale Challenge).

> *power of control in public interest also. Rather they must be mandated to do so.*" [emphasis mine][149]

In light of the above remarks by the court in *The Case Concerning Blue Whale Challenge*, the court's mandate to service providers in removing harmful content causing mental trauma such as the Blue Whale Challenge itself, is similar to how an operator/controller under EU Law can be directed to remove links to content mentioning personal data of data subjects. Although, a key difference here is that there was no individual involved and the web-pages did not actually publish personal data about an individual. On the contrary, a judicial authority directed removal of 'harmful contents' (akin to invoking the ground of public interest), while recording that service providers (who are addressed as operators/controllers in EU Data Protection Law) should regulate content displayed on their search results.

Having discussed three judicial decisions related to RTBF and the EU Law, let's move on to the *Puttaswamy* decision by the Supreme Court of India. The *Puttaswamy* decision, which contained six separate opinions, conceptualized multiple forms of privacy, including *informational privacy*, which protects the personal data of an individual. Given the fact that at least six judges (through judgments by Chandrachud, J., Nariman, J. and Kaul, J.) have expressly recognized the existence of the right to informational privacy and elaborated on the concept, it is a recognized fundamental right, derived from right to privacy.[150] While discussing the jurisprudence across the globe, the Supreme Court looked at the GDPR and the protections accorded to personal data in the western countries. It acknowledged, *inter alia*, the following aspects of informational privacy:

i. Individuals including children have access to social media and internet in the modern world, which leads them to leave footprints on the internet. Various forms of applications whether as simple as Bluetooth, or social media like Facebook, Instagram etc., or web downloading from emails, google and yahoo, are all ways in which data is being passed by children. Kaul, J. noted that children can be naïve and can often commit mistakes in their life. Therefore, he stated that the EU jurisprudence permits parents of such children to act as their legal guardian and request for removal of personal data in relation to their children.[151]
ii. Every individual should have the capacity to change his/her beliefs and improve as a person. The individual should not live in the fear that the

[149] *See id.,* ^21-22.
[150] *See* Puttaswamy, *supra* note 98, ^300-315, 328 (Chandrachud, J., for himself and Khehar, J., Agrawal, J. and Nazeer, J.), ^521 (Nariman, J.), ^621 (Kaul, J.).
[151] *See id.,* ^631-33 (Kaul, J).

view expressed by them will stay forever with them. Individuals should not be bound to the mistakes that they have committed in the past.[152]

iii. While an individual has inherent right under right to privacy, to control and restrict dissemination of information, this is not an absolute right and needs to be balanced with other competing interests depending on the circumstances. All six separate judgments in *Puttaswamy* support this position.[153]

While these are not the complete aspects of right to *informational privacy* discussed in the *Puttaswamy* decision, they do cull out aspects of RTBF after the *Google Spain* decision and the advent of GDPR in the EU. It is pertinent to note that none of the separate judgments in the *Puttaswamy* decision did not endorse or hold the position that there is a horizontal-application of the fundamental right to privacy between an individual and a non-state individual/person/entity (including the judgment by Kaul, J. as lucidly pointed out by Bhatia).[154] On the contrary, fundamental right to privacy in India is a right or "constitutional firewall"[155] that can be exercised by an individual against the state (i.e. vertical-application of fundamental right). While there are six separate judgments in *Puttaswamy*, none of them hold an absolute binding position (including the plurality opinion by Chandrachud, J.), since there was no majority of at least five judges joining or expressly concurring with the entire judgment given by another judge.

Nevertheless, there are numerous binding holdings or common observations of the *Puttaswamy* decision, which can be culled out while reading the six judgments jointly, as all judgments were concurring and there was not a single dissent. For instance, Chandrachud, J. (whose judgment was joined by Khehar, C.J.I., Agrawal, J. and Nazeer, J.) and Kaul, J. have both recognized the existence of a right to 'informational privacy', the individual's exercise of the right to privacy the existence of state surveillance, the limitations of privacy and the proportionality approach while adjudicating a case between competing state interests. Moreover, the

[152] *See id.,* ^634 (Kaul, J.).
[153] *See id.,* ^313, 325 (Chandrachud, J., for himself and Khehar, J., Agrawal, J. and Nazeer, J.), ^377-8 (Chelameswar, J.), ^419 (Bobde, J.), ^521, 526 (Nariman, J.), ^567 (Sapre, J.), ^629 (Kaul, J).
[154] Gautam Bhatia, *The Supreme Court's Right to Privacy Judgment – VII: Privacy and the Freedom of Speech*, Indian Constitutional Law and Philosophy, September 5, 2017, available at: https://indconlawphil.wordpress.com/2017/09/05/the-supreme-courts-right-to-privacy-judgment-vii-privacy-and-the-freedom-of-speech/ (Last Visited on May 25, 2021); Jayna Kothari, *The Indian Supreme Court Declares the Constitutional Right to Privacy*, Oxford Human Rights Hub, October 4, 2017, available at: https://ohrh.law.ox.ac.uk/the-indian-supreme-court-declares-the-constitutional-right-to-privacy/ (Last Visited on May 25, 2021).
[155] *See* Puttaswamy, *supra* note 98, ^375 (Chelameswar, J.), ^428 (Bobde, J.).

Nine-Judge Constitution Bench of the *Puttaswamy* decision had laid down various standards on the restrictions to the right to privacy, which can be divided into here major categories:

i. Chandrachud, J. laid down a 3-pronged test to privacy with respect to the legality, necessity and proportionality of the impugned action on the right to privacy. Kaul, J. agreeing with Chandrachud, J., added the requirement of procedural safeguards to the test.[156] Various scholars and authors believe that *Puttaswamy* decision mandates all four of these tests/requirements, upon a joint reading of the judgments by Chandrachud, J. and Kaul, J.[157]
ii. Chelameswar, J. borrowed the strict scrutiny standard from the United States to place certain extraordinary privacy claims at the *"highest standard of scrutiny"* which can be justified only in case of a *"compelling state interest"* while the other privacy claims can be justified by the just, fair and reasonable test. Based on the nature of the privacy interest claimed by an individual, limitations to privacy are to be identified on case-to-case basis. Nariman, J. elucidated the basis for this case by case analysis to be under the tests of the relevant fundamental right invoked. Bobde, J. supplemented this by requiring the privacy infringement to further be tested on touchstone of Article 21 – the procedure established by law.[158]
iii. Sapre, J noted that the restrictions to the right to privacy can be imposed by the state "*on the basis of social, moral and compelling public interest in accordance with law*" while acknowledging that the multifaceted nature of this right required determination on a case-to-case basis.[159]

As discussed in Part 3, the RTBF in the EU can be understood as a facet of privacy, the control-based theories of privacy, or dignity (which as per Bobde, J., Chandrachud, J. and Kaul, J. would encompass privacy).[160] If we

---

[156] *See id.,* ^325 (Chandrachud, J. for himself and Khehar, J., Agrawal, J. and Nazeer, J.), ^638 (Kaul, J.).

[157] *See* Gautam Bhatia, *The Supreme Court's Right to Privacy Judgment – VI: Limitations*, Indian Constitutional Law and Philosophy, September 1, 2017, available at: https://indconlawphil.wordpress.com/2017/09/01/the-supreme-courts-right-to-privacy-judgment-vi-limitations/ (Last Visited on May 25, 2021); Khamroi and Shrivastava, *supra* note 4, 111; John Sebastian & Aparajito Sen, *Unravelling the Role of Autonomy and Consent in Privacy*, 9 Indian J. Const. L. 23 (2020); Anujay Shrivastava and Yashowardhan Tiwari, *Understanding The Misunderstood: Mapping The Scope Of A Deity's Rights In India*, 10(1) WBNUJS International Journal of Law and Policy Review 27 (2021).

[158] *See* Puttaswamy, *supra* note 98, ^378 (Chelameswar, J.), ^426-7, 428.2 (Bobde, J.), ^525 (Nariman, J.).

[159] *See id.,* ^567-8 (Sapre, J.).

[160] *See id.,* ^41, 119 (Chandrachud, J. for himself and joined by Khehar, C.J.I., Agrawal, J. and Nazeer, J.), ^407, 411 (Bobde, J.), ^645-647 (Kaul, J.).

understand the RTBF as a facet of any of the foregoing human/constitutional values, it could become a part of Indian law subject to the aforementioned restrictions on 'right to privacy' in India. It is notable, however, that *Puttaswamy* decision does not discuss or mention the concept of RTBF or RTE in any of the six separate opinions.

Subsequent to the *Puttaswamy* decision, the India had formed a committee headed by Justice B.N. Srikrishna (retd.) (*a former Judge of the Supreme Court of India*), whose purpose was creating a draft data protection legislation, i.e. The Draft Personal Data Protection Bill, 2018 (*hereinafter* **First PDB**).[161] In the First DPDB, which is similar to the GDPR, the proposed section 27 expressly provides a limited statutory RTBF to every 'data principal' or 'person' as defined in the Bill, which enables the data principal to *restrict* or *prevent continuing disclosure* of their personal data. Had this legislation been adopted, it would have allowed for an individual ('data principal'; the equivalent of a 'data subject') to *horizontally* exercise a limited statutory 'right to informational privacy', 'right to control dissemination of data' or a RTBF (as stated in the First PDB), against *private entities* and *individuals* other than the 'state' (whose activities are already under a check due to the *vertical* application of the fundamental right to privacy between state and the individual, introduced in the *Puttaswamy* decision). An appropriate case where a statutory RTBF could have been beneficial to Indian citizens is the pending *WhatsApp Privacy Policy Case*.[162] In the backdrop of the First PDB, Khare and Mishra argued that it is important to avoid "over-broadness" while incorporating the protection under the RTBF.[163] They state that over-broadness is a situation where the wording of the law is too *vague* that it leads to violation of the constitutional provisions, such as Article 19(1) and Article 21 of the Indian

[161] Ministry of Electronics and Information Technology, Government of India, *Draft Personal Data Protection Bill, 2018*, PRS India, 2018, available at: https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018 (Last Visited on May 25, 2021).

[162] Chaitanya Rohilla v. Union of India & Ors., W.P.(Civ.) 677/2021 (Pending) (Delhi High Court) (*hereinafter* WhatsApp Privacy Policy Case). For a greater understanding of this case, *see* Abhijeet Shrivastava and Anujay Shrivastava, *WhatsApp Privacy Case: Does WhatsApp Perform A 'Public Function' Under Article 226 Of The Constitution?*, Constitutional Law Society of National Law University of Odisha, February 15, 2021, available at: https://clsnluo.com/2021/02/15/whatsapp-privacy-case-does-whatsapp-perform-a-public-function-under-article-226-of-the-constitution/ (Last Visited on May 25, 2021); Abhijeet Shrivastava and Rishav Sen, *WhatsApp's Privacy Policy, Public Policy And The Constitution*, NUJS Constitutional Law Society, December 3, 2020, available at: https://wbnujscls.wordpress.com/2020/12/03/whatsapps-privacy-policy-public-policy-and-the-constitution/ (Last Visited on May 25, 2021).

[163] *See* Komal Khare and Devershi Mishra*, Contextualizing Right To Be Forgotten In The Indian Constitution: Juxtaposing Right To Privacy And Right To Free Speech,* 3(2) CALQ 80 (2017) (*hereinafter* Khare and Mishra).

Constitution. If exhaustive definitions and a restrictive scope of the RTBF is incorporated into the First PDB, the issue of over-broadness could be avoided. Interestingly, the First PDB envisages not only penalties by way of fines, but also contains criminal imprisonment as punishment for violating rights of a person under this Bill. Consequently, the protection of *personal data* in India would stand at an enhanced stage compared to EU (while being invoked against a private entity or individual), owing to threat of criminal imprisonment.

In a surprising development, the First PDB was never adopted by India. Instead, India came up with a new Personal Data Protection Bill, 2019 (*hereinafter* **Second PDB**).[164] The key changes in the Second PDB have been eloquently discussed by Joseph and Basu (which needn't be reproduced here).[165] In a scathing criticism of the Second PDB discussing the problems introduced by the new Bill, Justice Srikrishna (*who headed the drafting the First PDB*) was quoted arguing that the Second PDB was 'dangerous' and had the potential to convert India into an 'Orwellian State'.[166] It has been noted that the Second PDB would enable the state to access 'non-personal data' (which has been classified as public, private or community).[167]

---

[164] *See* Ministry of Law and Justice, Government of India, *The Personal Data Protection Bill, 2019*, PRS India, 2018, available at: https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2019 (Last Visited on May 25, 2021).

[165] Vinod Joseph and Protiti Basu, *The Personal Data Protection Bill 2019 - A Comparison With The 2018 Bill*, Mondaq, December 19, 2019, available at: https://www.mondaq.com/india/data-protection/876842/the-personal-data-protection-bill-2019--a-comparison-with-the-2018-bill? (Last Visited on May 25, 2021). More insights can also be found in an article by PWC about this Bill, *see also* Ankit Virmani and Sonali Saraswat, *Data Privacy Bill 2019: All you need to know*, PWC, 2019, available at: https://www.pwc.in/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-you-need-to-know.html (Last Visited on May 25, 2021).

[166] *See* Megha Mandavia, *Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna*, Economic Times, December 12, 2019, available at: https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms (Last Visited on May 25, 2021).

[167] *Privacy Bill Will Allow Government Access to 'Non-Personal' Data*, The Wire, December 10, 2019, available at: https://thewire.in/government/privacy-bill-non-personal-data-voluntary-user-verification (Last Visited on May 25, 2021); Muskan Tibrewala and Pavan Kalyan, *Reconciling the Non-Personal Data framework with Database Protection in India – Part I*, IJLT, available at: ijlt.in/index.php/2020/12/13/reconciling-the-non-personal-data-framework-with-database-protection-in-india-part-i/ (Last Visited on May 25, 2021); Muskan Tibrewala and Pavan Kalyan, *Reconciling the Non-Personal Data framework with Database Protection in India – Part II*, IJLT, available at: http://ijlt.in/index.php/2020/12/13/reconciling-the-non-personal-data-framework-with-database-protection-in-india-part-ii/ (Last Visited on May 25, 2021).

While the Second PDB is yet to be adopted as a statutory enactment by the Indian Parliament, the Delhi High Court in May 2019 had expressly invoked the RTBF for the first time in Indian history (*as far as High Courts and the Supreme Court are concerned*), as a facet of *privacy*. In *Zulfiqar A. Khan*[168], a Single-Judge Bench of the High Court, comprising of Pratibha M. Singh, J., heard a prayer seeking to remove certain allegations of sexual harassment against the individual plaintiff which were posted in some online articles published by the defendant, The Quint, which is a private online news agency. The defendant had published the articles mentioning name of the plaintiff as a sexual harasser in wake of the #MeToo movement. The plaintiff requested the court to remove the articles until the disposal of the case, since the contents of the articles would tarnish his reputation and affect his life.[169] The court recognized the plaintiff's fundamental right to privacy, as well as its facets of RTBF and the 'right to be let alone'. [170] Consequently, it ordered the defendant to immediately remove the links uploaded on its website (including any modified versions and posts of the links on its social-media pages, such as Facebook) and co-operate with the plaintiff in this regard, until the case was disposed of. Moreover, the court allowed the petitioner to cite its order to direct any other person from publishing any similar content against him, until the case is disposed-off and report non-compliance of the order by any third parties to the High Court for further orders necessary.[171] While the court did invoke RTBF as a facet of privacy, it did not define the contours of the said facet and chose not to discuss any constitutional provisions, legislative provisions/bills or judicial precedents, which allow for the plaintiff to exercise RTBF in the manner used in the case. As discussed earlier, the fundamental right to privacy does not have a horizontal-application between two individuals/non-state actors. Consequently, the order in *Zulfiqar* permitting a use of RTBF (as a facet of privacy) against a non-state actor (such as the defendant, The Quint) is constitutionally flawed and impermissible in India. Interestingly, the way RTBF was invoked in this case, it has been similarly invoked by controllers to take down content describing pending judicial pronouncements on grave offences (including sexual assault cases) against a data subject in the EU, as demonstrated earlier by Lubis in her criticism.[172]

Importantly Khare and Mishra have pointed out that due to the constitutional and administrative law principle of "excessive delegation", the nature and scope of RTBF as prescribed in EU Law standards can be

[168] *Zulfiqar A. Khan v. Quintillion Business Media Pvt. Ltd.*, 2019 SCC OnLine Del 8494 (Delhi High Court) (*hereinafter* Zulfiqar).
[169] Id.
[170] Id.
[171] Id.
[172] Lubis, *supra* note 137.

substantially difficult to transpose into the Indian jurisprudence.[173] As discussed earlier, the RTBF under the GDPR entails an evaluation by a controller/private entity like Google/Yahoo to decide whether the link (or personal data) that is requested to be deleted/erased, satisfies any of the grounds for removal of personal data laid down in the GDPR.[174] Delegation of this power to evaluate the legality of RTBF to a private entity without any substantive guidelines is equivalent to giving these private entities a traditionally adjudicatory role of balancing two competing interests/rights, e.g. the right to privacy and the right to freedom of speech.[175] As clear from earlier discussions [in Part 5.1 and Part 5.3], private entities are guided by profit maximization, which greatly affects consideration of public welfare into account. Similar to what Divan[176] stated earlier, Khare and Mishra note that "*under the GDPR framework, private entities would tend to comply with the erasure*" rather than uphold the link or web-page, due to the enormous sanctions contemplated on non-compliance with the request. They argue that this would lead to a chilling effect by exercise of RTBF and its overriding effect on right to freedom of speech and expression, as well as freedom of press.[177]

In addition, assuming that the duty of evaluation of "*whether a successful RTBF claim exists and overrides a competing right of another person*", is delegated to an *executive body* under the state rather than private entities, it would still suffer from the vice of *excessive delegation* under the Indian Constitution, as issuance of unequivocal principles guiding the executive body by the legislature on how to decide which cases are legitimate enough to override the competing rights is necessary. Under the doctrine of excessive delegation under the Indian Constitutional Law and Administrative Law, it is a settled-principle that legislature has to mandatorily outline the 'standards for guidance' on an executive body's rule-making powers and to place legislative restrictions on its power.[178] Consequently, without any express legislative standards and restrictions on an executive body's rule making power, its adjudication of claims which involve RTBF and competing interests/rights would be impermissible under the Indian Constitution. Ramesh and Kancherla have also argued that the Indian constitutional jurisprudences on "freedom of speech" and RTBF

[173] *See* Khare and Mishra, *supra* note 163, 78-9.
[174] *See* GDPR, *supra* note 15, art 17.
[175] *See* Khare and Mishra, *supra* note 163, 78-9.
[176] Divan, *supra* note 138.
[177] *See* Khare and Mishra, *supra* note 163, 78-9.
[178] *See* V.N. Shukla, *Judicial Control of Delegated Legislation in India*, 1(3) Journal of The Indian Law Institute 357 (1959).

(deriving from 'privacy') are not truly analogous.[179] Thus, while there may be similarities in the supra-national EU's GDPR and India's nascent developments in privacy, as well as formulation of legislation to create a statutory RTBF, the scope of the two rights, the role of who decides whether a RTBF claim is successful against competing interests and the consequences arising from a failure to comply with a successful RTBF claim would be significantly different in the two jurisdictions.

7. Concluding Remarks:

The recognition of a RTBF/RTE in the EU has been of great significance to the world. It is indisputably due to the recognition of this right by the ECJ in *Google* Spain, academic writings and subsequently, through enactment of the GDPR by the EU Parliament, an accelerated growth of jurisprudence on protection of personal data has occurred across the globe. Practitioners like Singhvi have considered RTBF emerging from EU to be a 'human right'.[180] Given the significance of the GDPR, various legislatures, judicial authorities and scholars across the world have considered revising their own data protection laws to match the protections offered by the GDPR. Simultaneously, we must remind ourselves that RTBF is not an absolute right and there need to be necessary restrictions placed on it to safeguard competing interests/rights of other persons/entities and to avoid creation of a *chilling effect* on such competing interests/rights. A balancing exercise by a competent authority/judicial authority is a must in any jurisdiction, whether EU or India, when dealing with a RTBF claim.

In India, not only has the *Puttaswamy* decision itself referred to the GDPR[181], both the First PDB and Second PDB also incorporate a provision on RTBF. Therefore, it is clear from these facts that India is steadily recognizing a need for statutory remedies similar to that of RTBF in the GDPR, which is required to regulate processing of personal data and for individuals to make controllers/operators accountable (especially the non-

[179] Harikartik Ramesh and Kali Srikari Kancherla, *Unattainable Balances: The Right to be Forgotten*, 9(2) NLIU Law Review 411-2 (2020) (*hereinafter* Ramesh and Kancherla).

[180] *See* Saloni Singhvi*, Right To Be Forgotten: A Forgotten Right,* 9(2) WBNUJS International Journal of Legal Studies and Research 249-56 (2020).

[181] *See* Puttaswamy, *supra* note 98, ^636 (Kaul, J.). Interestingly, few academic sources relied on by Kaul, J. in his separate opinion involve a discussion on RTBF, even though the *Puttaswamy* decision does not mention RTBF. In addition, the Orissa High Court has recently recorded that the concept of RTBF and the law laid down in *Puttaswamy* are in sync, *see Subhranshu Rout v. State of Odisha*, 2020 SCC OnLine Ori 878, ^10. Although, importantly, as pointed out by myself elsewhere, the observations of the court on RTBF constitute an *obiter* and do not have precedential value, *see* Anujay Shrivastava, *Delhi High Court Order On Right To Be Forgotten: Analysis And Critique*, The Daily Guardian (New Delhi) June 1, 2021, 7 (*hereinafter* Shrivastava TDG).

state actors such as private entities). As pointed out earlier, while there are indeed many similarities between RTBF as present in the supra-national EU and as being conceptualized by the Indian Parliament or being invoked by various High Courts (both prior to and after the *Puttaswamy* decision), there are striking differences between the two jurisdictions, due to which a RTBF's nature, scope and adjudication/compliance will be significantly different in India compared to the existing EU Law and jurisprudence. Even, the consequences of non-compliance with a RTBF claim in both the jurisdictions are significantly different, with India focussing on greater criminal/penal consequences, compared to a focus on damages/civil nature of the RTBF in the EU. Consequently, a major takeaway for India would be to not copy or borrow the framework in the EU, but to build up its own version of RTBF in order to deal with the need of data protection law. In addition, it is important for incorporation of data protection provisions which keep in mind the informed 'consent' of individuals, especially when their data is being processed on a *day-to-day* basis. The need for a Data Protection Legislation in India may additionally stem from its international *erga omnes* obligations recognized by its judiciary.[182] Any future Data Protection legislations in India need to also ensure that a RTBF is *effective* and that its scope is not diluted enough to make it useless against competing interests of private entities or other actors (non-state or state).[183] For instance, incorporation of an express provision which allows a victim of revenge pornography[184] to be able to request expedited erasure of their personal data from entities/individuals controlling pornographic websites, search results of browsers, other virtual databases, whether through lawsuit, a governmental institution or directly approaching the concerned entity/individual would be highly desirable for the general public.

However, the fact that the Second PDB enables the state to store various forms of non-personal data highlight concerns for a state super-surveillance and the gross potential for misuse or danger arising from use of such data. Moreover, while use of RTBF as applied by the High Court in *Vasunathan*

---

[182] Devarshi Mukhopadhyay and Rahul Bajaj, *Locating The Right To Be Forgotten In Indian Constitutional Jurisprudence: A Functional-Dialogical Analysis*, 3(2) CALQ 57-60 (2017).

[183] *See generally* Navya Alam and Pujita Malkani, *Remembering to Forget: A Legislative Comment on the Right to be Forgotten in the Data (Privacy and Protection) Bill, 2017*, 7 NLIU Law Review 128-38, 138 (2018) (critiquing a draft Data (Privacy and Protection) Bill, 2017, which was introduced in Lok Sabha by Baijayant Panda, on grounds of inconsistency, lack of clarity (presence of ambiguity/vagueness) and limited scope of protection of personal data by the proposed RTBF within the draft Bill).

[184] *See* Smarnika Srivastava, *Can Copyright Protection Be Extended To Revenge Porn*, Lex Forti, March 28, 2021, available at: https://lexforti.com/legal-news/copyright-protection-revenge-porn/#_ftn36 (Last Visited on May 25, 2021).

decision [185] is commendable, there is also a need to avoid judicial incoherence in application of a RTBF until a data protection legislation is adopted by the Parliament. The Delhi High Court order in *Zulfiqar*[186] to restrain a non-state actor without the aid of any constitutional or statutory provision is problematic and an instance which demonstrates the need to avoid judicial incoherence. The order in *Zulfiqar* also fails to make a balancing of the "right to freedom of speech" of the victim or the world at large and the "right to privacy" of the accused.[187] Further, as demonstrated by Sridhar, recent decisions/orders of various Indian High Courts have contradicted earlier precedents, leading to judicial incoherence. [188] Additionally, a persisting great concern is India's delay in adopting an effective data protection framework, which meets the standards of proportionality. It is important that the Indian Parliament heeds to all of these concerns and comes up a data protection framework which not only allows for effective balancing in RTBF claims, but also addresses the concerns of state surveillance and enables individuals to make controllers/operators accountable. Until the scope of privacy and data protection mechanisms becomes adequate and effect, alternatives such as *obscurity*[189] may be beneficial to consider. In addition, while authors such as Kaushik believe that penalty or criminal punishment should not be adopted in India's future Data Protection law for 'mere deviations' from privacy expectations to, *inter alia*, promote free entry of smaller competitor firms, prevent concentration of market power and promote market welfare[190], they fail to outline what exactly would be the threshold to treat a *deviation* as a 'mere' or a 'major' deviation and who would be responsible for such a

[185] Vasunathan, *supra* note 101.
[186] Zulfiqar, *supra* note 168.
[187] *See* Ramesh and Kancherla, *supra* note 179, 411-2; Bitthal Sharma, *Right to be Forgotten: A Necessity for Progressive Realization of Rights*, CSIPR NLIU, April 7, 2021, available at: csipr.nliu.ac.in/technology/right-to-be-forgotten-a-necessity-for-progressive-realization-of-rights/ (Last Visited on May 25, 2021).
[188] Sriya Sridhar, *Walking the Tightrope of the Right to be Forgotten: Analysing the Delhi HC's Recent Order*, Spicy IP, May 15, 2021, available at: https://spicyip.com/2021/05/walking-the-tightrope-of-the-right-to-be-forgotten-analyzing-the-delhi-hcs-recent-order.html (Last Visited on May 25, 2021). For instance, Sridhar points out that a recent Delhi High Court order by a Single-Judge Bench of Pratibha M. Singh, J. contradicts the Gujarat High Court decision in *Dharmraj*, *see Jorawer Singh Mundy v. Union of India*, W.P.(C) 3918/2021 (Pending) (Delhi High Court), ^11. For a further critique of the Delhi High Court order, *see* Shrivastava TDG, *supra* note 181.
[189] *See generally* Woodrow Hartzog and Frederic D. Stutzman, *Obscurity by Design*, 88 Washington Law Review 385 (2013) (discussing principles of obscurity as an alternative to privacy and highlighting obscurity's benefits in light of privacy problems inherent in technology and internet).
[190] *See* Devansh Kaushik, *The Competitive Effects of Personal Data Protection Bill, 2019*, NLS Business Law Review, May 2, 2021, available at: https://nlsblr.com/the-competitive-effects-of-personal-data-protection-bill-2019/ (Last Visited on May 25, 2021).

classification. Should private entities, firms or individuals empowered to make this classification instead of Indian regulatory authorities, it could result in great potential for consumer harm and continuous deprivation of an individual's privacy over their personal data, unless such a private entity, firm or individual accedes to an individual's request for removal of their personal data or is directed by a regulatory authority to do so.

Finally, it is important to remember that while there can be several jurisprudential/theoretical conceptualizations of RTBF, it is extremely difficult or near-impossible to conceptualized RTBF as an independent right. As highlighted previously[191] the co-existence of RTBF and right to privacy (both of which purportedly protect 'personal data') raises concerns of theoretical indeterminacy where one right becomes redundant in presence of the other, if both are to be treated as independent of one another. The analysis in this article has demonstrated that the EU's attempt to bring GDPR without any express reference to privacy appears as an attempt to pass off RTBF as a new, separate and distinct right. In reality, a look at the EU jurisprudential history points out the fact that RTBF is applied right to privacy itself or a facet of right to privacy in the EU. This reiterates my argument that RTBF suffers from jurisprudential fallacies as: *first*, it is next to impossible to conceptualize it as an independent right, and *second*, co-existence of a RTBF and right to privacy (both rights being conceptualized and created to protect 'personal data') leads to theoretical indeterminacy. On a related note, it is indeed possible in future for legislators or scholars to demarcate the exact contours of a RTBF and distinguish it from the broader right to privacy, both of which protect personal data. Due to evolution in technology and jurisprudence, it is possible that the scope of RTBF may become narrower or broader depending on the needs of society. The fact that RTBF can be conceptualized as a derived facet of other values, such as autonomy (or 'control-based' theory of privacy) and dignity, show that RTBF in the near-future could be reimagined in a different form tomorrow compared to one that currently exists in EU or other nations. Although, such a task is challenging and would require co-operation between the legislators, practitioners, judges, academics, technology experts and even the common citizens across the globe, whose right over their personal data is at the very stake. In my final concluding remarks, I would like to acknowledge that while protecting one's personal data in the 21st century is becoming exceedingly difficult, the creation of data protection frameworks, debates and discussions by people of various streams across the world and growing education have helped us prepare to both know our rights, as well as learn ways in which we can protect our information and exercise control on its dissemination or availability.

[191] See discussion *supra* Part 4.