RIGHT TO BE FORGOTTEN: PRIVACY AND CYBERSPACE

Written by ***Sumedha Ganjoo***

Research Scholar/ Teaching Assistant, Bennett University, (Times of India), Greater Noida, Uttar Pradesh.

"They say we die twice. Once when the breath leaves our body, and once when the last person we know says our name"

- Al Pacino

ABSTRACT

The rule of privacy is encapsulated with the phrase "Right to be Left Alone"[i]. Social media turned this concept on its head and revolutionized the "Right to share all with the world". Every action may not have an opposite reaction and the boomerang effect to this is "free flow of personal information," a picture, video or even a message once set out to the online universe, cannot be retracted. In many instances, these tit bits, came back to haunt through social media. These instances led to the inception of the "Right to be Forgotten" movement.

Social media proves to be a more vengeful reaper than any law enforcement could envisage, in such instances of indiscretion. Henceforth, European Union("EU") decided to codify this right, also mentioned in 2012 Report carried out in full in the final approved document- "General Data Protection Regulation" or "GDPR (Regulation (EU) 2016/679). Interestingly when India is grappling with deciding on whether privacy is a fundamental right, the EU goes one step further to declare in the recitals to the GDPR "The protection of natural persons in relation to the processing of personal data is a fundamental right". As a natural progression therefrom, the GDPR reproduces the intent for the introduction of the "Right to be Forgotten". Article 17 of GDPR sets out the detailed provisions for the same. The said provision gives the right to data subjects, not just to erasure of personal data concerning them but to expeditiously erasure "without undue delay".

In India as well, the draft Personal Data Protection Bill, 2019, has a section on the Right to be Forgotten. But the proposed bill does not provide right to erasure. The bill has not yet been discussed in parliament and therefore, therefore the paper would assess its viability and suggest relevant changes.

Keywords- *Right to erasure, Right to be Forgotten, Data Privacy, Data Protection, GDPR.*

INTRODUCTION

Footprints in the sand of the internet are easy to forge but there is no tide to wipe them clean. They remain embedded in hidden cipher text and possibly in multiple locations. It is indeed easy to be heard and seen on the internet, but it is definitely not easy to erase those moments of indiscretion easily. Instances of a kindergarten teacher losing[ii] her job as her drunken photo was made viral, similarly a teacher with PhD in pedagogy losing her job as a result of a video of cocaine abuse going viral. The universe of Internet does not forget, even where law have acquitted persons[iii].

In January 2012, the European Commission submitted its proposal for "Regulation of the European Parliament and of the Council" on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[iv]. This was an upgraded version of the Data Protection Directive that had been holding sway since 1995. One of the primary inclusions in this proposal was the recognition of the "Right to be forgotten".

Till now in India, take down of defamatory or malicious content is possible through tortious civil actions. Criminal prosecution against publishing or transmission of defamatory content is dealt in Indian Penal Code (IPC). Recently Supreme Court of India that Intermediary Rules 2011[v], require intermediary to remove defamatory or vexatious content. However, in Section 79 of IT Act 2000 it is mentioned that intermediaries are required to comply with take down notices issued by court or appropriate authority and not merely on receipt of notice from

affected person. Following these rules individual grievances and complaints cannot be catered under Indian Law. The need for the hour is the much awaited Personal Data Protection Bill, 2019[vi] ("PDP Bill") issued on 26 August 2018 by the Ministry of Electronics & Information Technology ("MeitY") for public consultation along with the report of the Justice B.N. Srikrishna Committee on 'A Free and Fair Digital Economy[vii] – Protecting Privacy, Empowering Indians' ("Data Protection Committee Report") to be passed by the Parliament. The aforementioned PDP Bill includes a lot of hot issues that have created a buzz among companies and people affected by it. One such issue which has drawn a unique consideration of businesses and overall population is 'Right to be Forgotten' given under Section 27[viii] of the said bill. The said right has been consolidated in the PDP Bill on skirt of European Union's Data protection system through General Data Protection Regulation ("GDPR") with certain changes.

DIGGING TO PAST TO SEE FROM WHERE IT ALL STARTED

Legal counsellors, government officials, businessmen and academicians have roared about "the greatest danger to free discourse on the Internet in the coming decade," while Google said then and again that the right is a myth.

In March 2010, a Spanish citizen, Mr Costeja González, whispered to the Spanish National Data Protection Agency (AEPD)[ix] that when his name was entered in the Google internet database, the parts that originally appeared were pages of the 19 January and 9 March 1998 Barcelona paper La Vanguardia with a statement relating to a property of which he was joint owner in association proceedings. He mentioned, first, that La Vanguardia be required either to adjust those pages with the goal that the individual information identifying with him never again showed up, and furthermore that Google ought to be required to evacuate or hide the individual information identifying with him so they stopped to be incorporated into the indexed lists. He expressed that the connection procedures had been completely settled for various years and that reference to them was currently totally insignificant.

That raises a point that we feel is worth emphasizing. Off probability the data is inaccurate or insufficient, the source of the information has the right of receiving its modification or eradication from the database controller. Off chance the data, however reliable, is in violation of criminal law on a site — may be child pornography entertainment — the information controller has an undertaking to remove the link with it. The comparison refers to information on a site which are oppressive or contradict social equality[x]; web crawlers constantly get, and follow up on, solicitations to evacuate material which are allegedly in breach of copyright. For this situation there was no recommendation that the data was wrong; and a long way from being illicit, the production of the data by La Vanguardia occurred on the request for the Spanish Ministry of Labor and Social Affairs and was proposed to give most extreme attention to the sale so as to verify whatever number bidders as could be expected under the circumstances. This case, and our appeal, are concerned distinctly with facts which are actually on a platform and which the facts subject would lean toward not to be effectively accessible via a link to their name on an internet searcher.

The objection against Google was maintained. The AEPD thought about that administrators of search engine are dependent upon information security enactment given that they complete information preparing for which they are capable and go about as intermediary in the data society. Google took the issue to the Audiencia Nacional (the Spanish High Court), which alluded to the Court of Justice three inquiries on the elucidation of the Directive for primer decision.

TERRITORIAL EXTENT OF THE DIRECTIVE

The main inquiry questioned whether the territorial scope of the Directive reached out to Google's exercises in Spain. Promoter General Jääskinen exhorted it to do so, and the Court pursued its advice. The reach of the EU information security enactment in this way extends to cover EU and non-EU associations with EU activities — even where such tasks exclude the handling of information, as Google Spain SL does. This has been portrayed by Morrison and Foerster, a global law firm with one of the world's largest security and information security rehearsals, as "an extremely broad understanding of the regional scope of the Directive [which]

has little premise in the current wording of Article 4.1." We can see that this may pose problems with a worldwide relationship such as Google, which works in various wards outside the EU as well as within the EU, but it does not appear to us to create difficulty with UK data security regulations[xi].

IS AN INFORMATION CONTROLLER A SEARCH ENGINE[xii]?

In its second question, the Spanish court sought a ruling on whether Google's exercises as a search engine made them a "controller" of individual information distributed by outsiders on web pages. The problem here, as emphasis was called by Advocate General (Miyashita 2016), is that:

"At the point when the Directive was received the World Wide Web had scarcely become a reality, and search engine were at their incipient stage. The arrangements of the Directive just don't consider the way that tremendous masses of de-centrally facilitated electronic records and documents are available from anyplace on the globe and that their substance can be duplicated and broke down and scattered by parties having no connection at all to their creators or the individuals who have transferred them onto a host server associated with the web."

A "controller" is characterized by Article 2(d)[xiii] of the Directive as "the characteristic or legitimate individual … which alone or together with others decides the reasons and methods for the handling of individual information". The Advocate General and the Court thusly needed to choose whether that definition, drafted with no idea being given to web search tools, could be extended to incorporate them. The Advocate General contended that:

"the general plan of the Directive … and the individual commitments it forces on the controller depend on the possibility of obligation of the controller over the individual information prepared as in the controller knows about the presence of a specific characterized classification of data adding up to individual information and the controller forms this information with some goal which identifies with their handling as close to home information. "

The Court in this way decided the administrator/operator must be viewed as the "controller" of the data prepared/processed by the internet searcher.

THE RIGHT TO BE FORGOTTEN

On the off chance that the Court had pursued the Advocate General's Opinion on the subsequent inquiry, the third question on the privilege to be overlooked would not have emerged, since the privilege to acquire correction or deletion of information is accessible just as against the information controller. But since the Court chose Google[xiv] ought to be treated as an information controller, the third question must be replied. It was outlined by the Court as soliciting whether the applicable arrangements from the Directive ought to be deciphered "as empowering the information subject to require the administrator of an internet searcher to expel from the rundown of results shown following a hunt made based on his name connects to website pages distributed legally by outsiders and containing genuine data identifying with him, on the ground that that data might be biased to him or that he wants it to be 'overlooked' after a specific time."

Judgment[xv]

The court scotched such talk — just because, it built up a privilege in this space by maintaining (and apparently expanding) the AEPD's unique judgment. It chose that search was information handling under the (somewhat wide) definition in the Directive — the information is gathered, put away, recovered, revealed, etc. All things being equal, the handling occurs in the US by Google Inc. — what has that have to do with Google Spain? To start with, the court contended that Google Spain was a foundation in the EU (no one contested this), thus Spanish law applied to it. It at that point proceeded to contend that the preparing (in the US)[xvi] was done with regards to the exercises of Google Spain on the region of the part state Spain that were "planned to advance and sell … publicizing space offered by the web search tool, which serves to make the administration offered by that motor productive." Those promoting exercises made a connection between Google Spain and the search engine's information handling; the court likewise contended that the Directive is intended to cover the information assurance privileges of EU residents inside the EU[xvii], thus it will undoubtedly translate the different ideas broadly. Most questionably, the court dismissed Google's third guarantee that is anything but a

controller. This is a dependable position, conveying with it stringent information assurance duties; it pursues this is a key piece of the judgment.

Google[xviii] contended that, regardless of whether it forms individual information, it sees no difference amongst individual and non-individual information, which land at its entryway in a heedless and irregular manner. It's a latent middle person, has no association with the information or the website admins distributing it, and has no critical command over the substance. The Advocate General concurred — to be a controller, "the information handling must appear to him as preparing of individual information, that is 'data identifying with a distinguished or recognizable regular individual' in some semantically pertinent way and not a negligible PC code. "But rather the court disputed. The search engine "decided the reasons and methods for preparing" inside the setting of the exercises of Google Spain. This preparing is independent from that performed by the outsider website admins, and comprises in making "an organized review of the data" identifying with the individual looked for, which couldn't be made without the internet searcher. Again, it felt that full information security for EU subjects must be furnished if the definition was translated with a wide extension.

At long last, the court chose that Google had no duty to contact outsider website admins to disclose to them something had been de-recorded, and that if the data was legitimately distributed (and along these lines genuine), the data shouldn't be expelled from the Internet. The key security intrusion is the plausibility of making an outline about an individual; the data protested should possibly be de-recorded in this way if the pursuit's watchwords are the person's name. My security is repudiated undeniably more when somebody scanning for "my name" finds that I submitted some minor however humiliating offence, than when she looks for the wrongdoing and finds my name among the culprits, in light of the fact that in the previous case she's plainly inspired by me by and by, though in the last she's most certainly not. There are additionally protections when the individual included is an open figure, whose private life might be of real open intrigue[xix].

RIGHT TO BE FORGOTTEN UNDER GDPR

The most questionable and maybe generally taking steps to search indexes is the GDPR's Article 17[xx] which classifies the privilege to be forgotten. Normally alluded to in French as droit á l'oubli, the privilege to be forgotten has a long and complex history inside European law. Initially droit á l'oubli started as an idea for previous hoodlums who had served their sentences in jail and were liberated. The thought was that since they have paid their notorious obligation to society, they were qualified for a new begun unrestricted by their criminal past. Along these lines, their past criminal narratives were "crushed," and they started their lives again as beneficial individuals from society. American law[xxi], on the other hand, has no such recorded defense for evacuating an individual's past, criminal or something else. American law has constantly supported that free discourse took into consideration an individual's criminal past to turn out to be a piece of open record due to the need to secure society. It is this conflict of lawful and philosophical qualities that supports the right to be forgotten issue.

Article 17 of the GDPR[xxii] states that a client has a "privilege to get from the controller the deletion of individual information identifying with them and the abstention from further spread of such information, particularly in connection to individual information" when there is no utilization for the information or, all the more significantly, when the "data subject" chooses the person in question never again needs the data open. In addition, under Article 17 the controller not just needs to expel information on destinations they are responsible for yet should likewise "make every single sensible walk, including specialized measures… to illuminate outsiders which are handling such information, that an information subject solicitations them to eradicate any connects to, or duplicate or replication of that individual information."

This third party can be another web search tool or web organization, yet it likewise incorporates other individual clients, for example, Facebook companions or Twitter devotees. Under this guideline, retweets, sharing, remarks, re-posting, or posted remarks establish spread of individual data. Search engines and online networking outlets are required to advise these clients regarding this solicitation, yet in addition take specialized measures to expel these particular information demands about explicit bits of information[xxiii]. These information Controller can be very specific. Controller could incorporate the expulsion of an image, post, remark, or label that the information subject never again needs scattered on the Internet. Controllers are required to evacuate data when mentioned, yet they are additionally required to

confine access to information when the data is no longer utilized by the controller or if there is some inquiry with respect to whether the information is an honest portrayal of the information subject (Article 17). There are exemptions to this standard for required expulsion.

The GDPR Article 17 takes into account controllers not to evacuate information when it includes free express or when "open intrigue, for example, issues of well-being, logical research, lawful prerequisites, or authentic critical protection emerge that requires the upkeep of information. Be that as it may, these special cases are incredibly constrained and subject to the audit of the European Commission and European Data Protection Board. Researchers bring up that necessary evacuation or restricted access to information gives a strategic issue to many pursuit engines. It initially requires non-E.U. based organizations[xxiv] to cling to E.U. guideline in their support and advancement of overall sites and web indexes[xxv]. Second, and maybe generally hazardous, is that these guidelines direct organizations to react quickly to the solicitations of individual clients who at some random time may have little, complex evacuation demands that are hard to track and costly to expel.

The rules give thirteen regular criteria to assess an expulsion demand. These criteria look to[xxvi]

1) Whether the data is recorded when looking at an individual's name;
2) What is the client's "open-life" status;
(3) The age of the person specifying that material;
(4) The integrity of the personal data;
5) How much data about a person exists online;
(6) Whether the personal data are "touchy" or "dirty" data;
7) Is the current data for each individual;
8) Is the data "causing bias" about the individual
9) Does the data "endanger" the individual;
10) Is the data intentionally placed to the internet, or was it something that a person might expect to stay private?
11) The data was placed online by a columnist or news outlet;
12) Was the electronic data collection in spite of the fact that it was constitutionally necessary to be opened;
13) Is Network details focused on illegal activity or misconduct.

While these rules don't give dispositive responses to what can be expelled on the web, they do give a general feeling of what the Court of Justice planned when they saw a privilege as overlooked law exists. Progressively newsworthy data, for example, a significant criminal conviction, and data one would hope to discover on the web, for example, an expert connection, would almost certainly stay online regardless of whether a client mentioned that data be expelled. Similarly, data about a minor, individual data about medical problems, or slanderous proclamations about an individual would probably be the sort of data that would be evacuated whenever mentioned. These rules represent the European Union's endeavor at finding some kind of harmony between newsworthy data with open intrigue and private data that is close to home.

RIGHT TO BE FORGOTTEN IN INDIA

In opposition to prominent reports, courts have yet not perceived the "right to be forgotten" under Indian law. Be that as it may, there are valid justifications to have one's name separated from open records in light of a legitimate concern for security and comparable worries, as has been done with regards to casualties of rape. It's anything but an all-encompassing right that ought to essentially be accessible to all regardless of setting. Without any security enactment, it is bound to be a judicially created cure in explicit cases.

In order to understand Right to Be Forgotten 's situation in India, the status of the right to privacy needs to be investigated. Although the constitution did not initially give the right to privacy, a progression of Supreme Court decisions recalled that right as a key right under Article 21[xxvii] of the Indian Constitution. The Right to Be Lost has ignored the Indian Legal System's cornerstones to receive the recognition. The key right notification can be found in Section 228A of the Indian Penal Code and Section 23 of the POSCO Act, which restricts its scope to sexual offences against individuals remembering their impotence against women and children. The legal framework has managed to combine some of the highlights through criminal legislation and the Information Technology Act, 2000[xxviii]. Section 43A of this demonstration requires Corporate Body to carry out sensible practices to ensure individual

information is provided. A progression of late decisions on the issue, however, has raised appropriate issues regarding its recognition as a lawful right by drawing relationship from western patterns.

The judgment of the Karnataka High Court, which affirmed the right of the lady to be forget in a criminal case reported against her synchronous to conjugal issue, provided an opportunity to think about this right. This is still huge, regardless of its analysis, given that there are no classified laws on information security in India. The wandering outlook on high courts in this matter is evident from Gujarat High Court's judgment[xxix] denying the privilege of being ignored by bringing together its dissuasive regard for the 'reportable' question. Right now, the Delhi HC is managing a case including the demand for expulsion from an online database judgment whose choice would be a significant path for observing the Indian legal point of view on right to be forgotten. This demonstrates lack of clarity regarding the right to be overlooked in India. This requires an organized legal system that complies with the laws of information insurance.

The discussions are not just restricted to search engine responsibilities. Looking from the viewpoint of India, it calls for consideration, for example, of the new rights identified in the fight with the right to be forgotten. Likewise, there might be examples of its abuse as seen where a Rajya Sabha member acquired directive against a site for not publishing two articles. The premise of authorization of the Right is by all accounts the idea of data. Incredibly delicate data influencing individual existence needs security from pointless dispersal. This proposed right disregards prior and a perceived noticeable constitutional right, i.e., right to freedom of speech and expression.

In any case, both these rights aren't outright and dependent upon specific confinements. What's more, considering the equivalent stature of both the rights, it ought to be left to the judiciousness of court while arbitrating to think about whether it has drawn an ideal parity and not supported one for the other. The avocation for this contention lies in the way that the right to speak freely involves certain obligations (negative rights) include insurance of notoriety of others. For example, an issue concerning open intrigue will liable to have right to information exceeded against right to free discourse. Moreover, matters concerning divorce questions bring about divulgence of imperative individual data in the official courtroom and the spread of which may influence of interests of one of the parties. Providing the Right to Be Forgotten

involves sensibly checking right to free discourse[xxx]. One of the inventive approaches to catch the issue is the private understandings among web indexes and information controllers particularly legitimate for India which doesn't have any information/data protection enactment. Rather than superfluous enactment, the data controllers can have a private setting whereby they can address the issues concerning distribution of unimportant or lacking data, imposition of rules governing the same can be avoided.

Indian draft bill

The B.N. Srikrishna Committee report[xxxi] has laid huge accentuation on getting the assent of a person to process and utilize individual information. The committee said assent/consent must be "educated/informed", "explicit" and "clear", and should be fit for being pulled back as effectively as it was given.

The draft Personal Data Protection Bill, 2019[xxxii], has a segment on the Right to be Forgotten. Yet, the proposed bill doesn't give right to eradication.

Section 27[xxxiii] of the bill has rattled off three situations in which an individual will reserve the "right to confine or avert proceeding with revelation of individual information" or the right to be forgotten, it could be said;

(a) This will be material if information exposure is never again fundamental/useful,
(b) The consent to utilize information has been pulled back or
(c) When information is being utilized in opposition to the arrangements of the law.

A mediating official should decide the materialness of one of the three situations. The official will likewise need to discover that the right of the person to limit utilization of his/her information supersedes the right to free speech or right to information of another person.

While there is no outright right to eradication/erasure of information in the proposed law, the bill will soon experience a parliamentary procedure of discussion/debate which might lead to few changes in the bill before it becomes law of the land.

CONCLUSION

In the present socio-political conditions, to comprehend that a data protection enactment reflecting the EU mandates won't serve the requirements of our nation. This is because of the accompanying reasons; Firstly, the privacy laws in India is distinctly not the same as the EU. By this, I imply that privacy as a perfect notion seen in India is seen under an alternate light when contrasted with western nations fundamentally because of the change in culture. The EU specifically give more noteworthy significance to the idea of "independence" while we are an intrinsically "aggregate" society. Indians esteem both the individual and social part of privacy settled in a solid culture of trust. Therefore, the significance appended to privacy can't be applied to the two locales in a similar sense.

Also, simple affirmation of the way that Right to be forgotten exists doesn't make the position of law strong on the point of data protection. There is no suggestion that the State will presently take a gander at it as an approaching authoritative prerequisite. As the years progressed, different bills with respect to privacy and information/data protection, specifically, have been pending before the Parliament. Be that as it may, none of these made through as Acts. As of late as well, a MP moved a private part's Bill in the Lok Sabha in consonance with the progressing privacy hearings. However, dazzle use of laws of another nation will bring about poor results and failure of legal enforcement by judiciary.

Thirdly, giving all forces to outsiders to settle on whether specific data ought to be expelled or not will undermine the job of the State. The outsiders will go about as private managerial bodies despite the fact that they are benefit making associations. This may prompt confusion, consequently reducing the privilege to data which is essential to the Indian culture.

Finally, numerous nations in the EU are currently campaigning to expel joins from the worldwide space notwithstanding the area explicit areas. For example, France is currently requesting that Google expel specific connections from google.fr as well as from google.com

which is an obstacle to different wards. At this point, India is in a monetarily flourishing position and this sort of authoritative conduct can have grave repercussions on exchange and advancement.

The Delhi HC has included Google Inc and Google India to a suit including the de-posting of a connection which showed candidate's wife involvement in a criminal case. The candidate would not like to be related with a case that could influence his planned employment. This case will be a significant hearing in anticipating the fate of data protection system/framework. In expectation, I trust that the legislators accept this as a challenge to give shape to the Right to Be Forgotten in a genuinely Indian manner/conditions.

All in all, I might want to state that albeit Indian judges have at a few events, returned to the EU orders, it is unreasonable to apply them to the Indian setting because of the contentions progressed in this paper. In this way, the state of affairs requires the acknowledgment of the right to privacy as an intrinsic right, simply after which the governing body may raise the matter of data protection laws.

REFERENCES

Books

1. N.S. Nappinai (2017) *Technology Laws Decoded* (Lexis Nexis).
2. Javid Ahmad Dar (2019) *Privacy and Data Protection Laws in India, U.S.A and E.U.*
3. M S Helen Wong MBE (2018) *Cyber Security Law and Guidance.*
4. Amar K Sundram Anghrija Chakraborty, Ashima Obhan (Author) (2020) *Data Protection Laws Demystified*
5. G. E. Kennedy, L. S. P. Prabhu (2017) *Data Privacy Law: A Practical Guide*

ENDNOTES

[i] Justice Brandies.
[ii] Giancarlo F. Frosio, *Right to Be Forgotten: Much Ado About Nothing*, SSRN ELECTRONIC JOURNAL (2017)
[iii] (Shackelford and Craig 2014)
[iv] House of Lords - European Union Committee, *EU Data Protection law: a "right to be forgotten"?*, HL PAPER 40 (2014)
[v] Alok Prasanna Kumar, *"Right to be forgotten" in Indian law*, 52 ECONOMIC AND POLITICAL WEEKLY 10–11 (2017)
[vi] Chapter Ii et al., *India THE PERSONAL DATA PROTECTION BILL, 2018 CHAPTER I PRELIMINARY*, (2018), http://www.prsindia.org/uploads/media/Data Protection/Draft Personal Data Protection Bill, 2018.pdf
[vii] Anirudh Burman, *Will a GDPR-Style Data Protection Law Work For India?*, MAY 2019 (2019)
[viii] Chapter Ii et al., *Introduction*, 4 EUROPEAN DATA PROTECTION LAW REVIEW 1–20 (2018), http://petroleum.nic.in/docs/Notification issued for introduction of BS IV compliant four wheel motor vehicle.pdf
[ix] 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 981–1072 (2018)
[x] European Commission Justice, *Factsheet on the " Right to be*, PROTECTION OF PERSONAL DATA (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
[xi] Cayce Myers, *Digital Immortality vs. "The Right to be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy*, 16 ROMANIAN JOURNAL OF COMMUNICATION AND PUBLIC RELATIONS 47 (2016)
[xii] Hiroshi Miyashita, *BRUSSELS PRIVACY HUB THE " RIGHT TO BE FORGOTTEN " AND SEARCH ENGINE LIABILITY*, 2 (2016), http://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N8.pdf
[xiii] House of Lords - European Union Committee
[xiv] Post
[xv] J Rosen, *Google knows too much about you*, 64 STANFORD LAW REVIEW ONLINE 88 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten?em_x=22
[xvi] Myers
[xvii] Post
[xviii] Miyashita
[xix] Policy Brief, *The " Right to be Forgotten ": Remembering Freedom of Expression*, (2016)
[xx] O F T H E Council, *(Text with EEA relevance)*, 2014 (2016)
[xxi] Myers

[xxii] The data subject shall have the right to obtain from the controller, without undue delay, the erasure of personal data relating to him or her and the controller shall be obliged to erase personal data without undue delay where one of the following grounds applies:

a. Personal data relating to the reasons for which they were obtained or otherwise stored are no longer required;

b. The data subject shall withdraw the consent on which the processing is based pursuant to point (a) of Article 6(1) or point (a) of Article 9(2), and where there is no other legal basis for the processing;

c. The data subject objects to the processing referred to in Article 21(1), and there are no overriding legitimate grounds for the processing or objects of the data subject to the processing referred to in Article 21(2);

c. The personal details is stored unlawfully;

Personal data shall be erased in order to comply with the legal obligation laid down in Union or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Where the controller has made personal data public and is obliged to erase personal data pursuant to paragraph 1, the controller shall take reasonable steps, including technical measures, to inform the controller that the data subject has requested the erasure of such controllers. Paragraphs 1 and 2 shall not extend to the degree required for the collection of:

To exercise the right to freedom of speech and of information;

a. For the execution of a legal duty involving the collection by Union or Member State statute to which the controller is subject, or the completion of a function undertaken in the public interest or the exercising of an official authority in the controller 's possession;

b. Pursuant to points (h) and I of Article 9(2) and Article 9(3), for reasons of public interest in the field of public health;

c. For archiving purposes of the public interest, for scientific or historical research purposes or for statistical purposes of compliance with Article 89(1), in so far as the right referred to in paragraph 1 is likely to make the achievement of the goals of that processing difficult or seriously impaired; or

d. For the development, practice or protection of legal claims.

[xxiii] Rosen

[xxiv] Frosio

[xxv] Kieron O'Hara, *The right to be forgotten: The good, the bad, and the ugly*, 19 IEEE INTERNET COMPUTING 73–79 (2015)

[xxvi] House of Lords - European Union Committee

[xxvii] Faiza Bhandari, Vrinda; Kak, Amba; Parsheera, Smriti; Rahman, *An Analysis of Puttaswamy : The Supreme Court ' s Privacy Verdict An Analysis of Puttaswamy : The Supreme Court ' s Privacy Verdict*, (2017)

[xxviii] M. A. Yadugiri & Geetha Bhasker, *The Information Technology Act, 2000*, ENGLISH FOR LAW 482–511 (2011)

[xxix] Bhandari, Vrinda; Kak, Amba; Parsheera, Smriti; Rahman

[xxx] Commitee, *White Paper of the Committee of Experts on a Data Protection Framework for India*, WHITE PAPER (2017), https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

[xxxi] Fair Digital Economy et al., *Introduction*, 4 EUROPEAN DATA PROTECTION LAW REVIEW 0–28 (2018), https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

[xxxii] Ii et al.

[xxxiii] Right to Be Forgotten. — (1) The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure— (a) has served the purpose for which it was made or is no longer necessary; (b) was made on the basis of consent under section 12 and such consent has since been withdrawn; or (c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature. (2) Sub-section (1) shall only apply where the Adjudicating Officer under section 68 determines the applicability of clause (a), (b) or (c) of sub-section (1) and that the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen. (3) In determining whether the condition in sub-section (2) is satisfied, the Adjudicating Officer shall have regard to— (a) the sensitivity of the personal data; (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life; (d) the relevance of the personal data to the public; and (e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented. (4) The right under sub-section (1) shall be exercised by filing an application in such form and manner as may be prescribed. (5) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2) does not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of that

order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (3).