NLIU LAW REVIEW

VOLUME VII

JULY 2018

NATIONAL LAW INSTITUTE UNIVERSITY

KERWA DAM ROAD, BHOPAL - 462 044 (M.P.)

The NLIU Law Review is published by the students of National Law Institute University, Bhopal, India.

The NLIU Law Review publishes material on subjects of interest to the legal profession. It invites unsolicited manuscripts for publication. Such manuscripts should be sent in MS Word (.docs format) to *lawreview@nliu.ac.in* All citations and text generally conform to The Bluebook: A Uniform System of Citation (20th ed. 2015).

Recommended form of citation:

(2018) 1 NLIU L. Rev. <page no.>

ADVISORY PANEL

PEER REVIEW PANEL

General Student Body of NLIU Law Review 2018-19

EDITOR-IN-CHIEF

Avani Mishra

CONTENT REVIEW BOARD

Board Heads – **Aishwarya Nair and Prabal De**

Fourth Year Members
Akshay Sharma, Kashish Mahajan, Nidhi Kulkarni, Prabal De and Saara Mehta

Third Year Members
Charu Vyas and Doorva Tripathi

Second Year Members
Anoushka Ishwar, Diya Gupta, Rayana Mukherjee, Ritwik P.Srivastava and Saavni Kamath

TECHNICAL REVIEW BOARD

Board Head – **Udyan Arya**

Fifth Year Members
Rohini Dayalan, Shantanu Pachauri and Varnika Taya

Fourth Year Members
Farah Naeem, Iravati Singh, Ravleen Kaur, Simranjeet and Utsav Mitra

Third Year Members
Harita Putrevu and Tanvi Prabhu

MANAGERIAL BOARD

Board Head – **Divyam Sharma**

Fourth Year Members
Aryan Gupta, Dhruv Khurana and Nirjhar Sharma

Third Year Members
Saumya Agarwal and Suyash Bhamore

Second Year Members
Kartikey Bansal, Shiuli Mandloi and Utsav Garg

CONTENTS

MESSAGE FROM THE PATRON-IN-CHIEF

Justice Hemant Gupta
CHIEF JUSTICE

191, South Civil Lines,
JABALPUR - 482 001
Tel. (O) 2626443
(R) 2678855
2626746
Fax 0761-2678833

2nd August, 2018

MESSAGE

I am extremely proud to announce the publication of the seventh volume of NLIU Law Review to the legal community. The NLIU Law Review aims to serve as a forum for promotion of discourse on contemporary and pressing legal concerns at both the national and international levels. Since its inception this student helmed publication has sought to cultivate a style of scholarship that explores both the theoretical and the practical concerns of the legal world. To ensure this, it has consistently employed stringent evaluation techniques with emphasis on contemporary relevance, critical thinking, originality and lucidity of prose.

This year's issue revolves around the theme of '*Data Protection and Privacy*' which was chosen with a view to provide a comprehensive outlook on the complex nature of personal data protection across the globe. This issue not only aims to address problems which arise in this multifarious field but also seeks to provide unique and constructive solutions to tackle the same.

I extend my congratulations to Prof. (Dr.) V. Vijayakumar and Prof (Dr.) Ghayur Alam for another successful publication and commend the student members of this Review for their work and dedication. May the Editorial Committee maintain the same vigour in the coming years. I hope that students, academicians, lawyers and judges and all other readers will find this publication stimulating and beneficial.

(Hemant Gupta)

MESSAGE FROM THE PATRON

NATIONAL LAW INSTITUTE UNIVERSITY

Ref. No. ...../NLIUB

Prof. (Dr.) V. Vijayakumar
M.A., M.L., M.Phil., Ph.D.
Director

Date : 3/8/2018

MESSAGE

It gives me immense pleasure to present Volume VII of the NLIU Law Review to our readers. Inspired by recent developments in the field of technology and development, as well as the wave of support for personal rights like *Puttuswamy* judgment, this volume aims to highlight and facilitate a discussion on a pressing socio legal issue – '*Data Protection and Privacy.*' I sincerely hope that the contents of this volume will infuse new perspectives to this highly contentious topic, in terms of policy, law and its implementation.

The NLIU Law Review has since its inception, served as a platform for academicians, lawyers, students and policy-makers alike to contribute to the legal discourse on contemporary issues. This journal is also expected to encourage originality through qualitative legal research by rigorously evaluating the submissions on grounds such as contribution to knowledge and contemporary relevance.

I would like to thank the Patron-in-Chief of the Law Review, Hon'ble Shri Justice Hemant Gupta, Chief Justice, High Court of Madhya Pradesh for his invaluable guidance in this endeavour. I would like extend my appreciation to Prof. (Dr.) Ghayur Alam for successfully supervising the publication of this issue by providing constant and helpful inputs to the student editors. I congratulate and commend the Editorial Team on their hard work in bringing out this issue and hope that their enthusiasm only grows with each upcoming issue. Lastly, I look forward to your feedback on the contents of this issue as well as our editorial policy, as they would inspire to improve and better the publications of NLIU in general and NLIU Law Review in particular.

(V. Vijayakumar) 3/8/18

University established by Madhya Pradesh Act No. 41 of 1997

Kerwa Dam Road, Bhopal - 462 044, (M.P.) India
Tel : 0755 - 2696965, 2696970 (O) Ext.-109, Fax : 0755 - 2696724
E-mail : director@nliu.ac.in, vijayakumar@nliu.ac.in, Visit us at : www.nliu.ac.in

A NOTE FROM THE FACULTY ADVISOR

This is a Special Volume of the NLIU Law Review on *'Data Protection and Privacy.' Since Justice K S Puttaswamy v. Union of India (SC: August 24, 2017),* the discourse on data protection and privacy started getting unprecedented attention from all sections of the society, including media and academics. Our students decided to bring this Special Volume and succeeded. The students have earned appreciation hence they deserve our congratulations. I hope that they will make further endeavour to promote debates and discussions on topical issues. Bringing a Law Review is a joint enterprise of the contributors and the managerial and editorial teams. Every contributor and every member of NLIU Law Review deserves our unconditional gratitude.

Our Patron-in-Chief, Hon'ble Justice Hemant Gupta, the Chief Justice of the Madhya Pradesh High Court, has always been a source of inspiration for us. We express our unbounded gratitude to the Chief. Prof. (Dr.) V. Vijayakumar, who has joined NLIU as the Director in May 2018. He is a teacher with more than four decades of teaching and administrative experience. Perhaps, he is the only Director (Vice-Chancellor) of a National Law University having the longest experience of working in a National Law University system. Given his wide and long experience, we the members of the NLIU family have a lot of hope and expectations from him. In a period of less than three months at NLIU he has been able to demonstrate that

NLIU has the potential to become a, if not the, centre of excellence in academics. We express our unbounded gratitude to him.

The success of this Volume lies in the quality of criticism that it may be able to generate. The readers are requested to send their comments, criticism, and suggestions on the articles published herein. We will publish the comments and criticism in the next Issue.

Prof. (Dr.) Ghayur Alam
Professor in Business and Intellectual Property Laws
National Law Institute University

EDITORIAL NOTE

The VII[th] volume of the NLIU Law Review, the journal's second thematic issue, presents a fascinating blend of divergent opinions on topics closely connected to the current state of *Data Protection and Privacy* on both a national and international scale. The following articles aim to chronicle these developments and comprehensibly address several of these concerns and attempt to provide realistic solutions.

In *Data Protection – Protection of what, Protection from whom & Protection for whom - An Analysis of the Legal and Judicial Provisions in India and abroad,* the author takes the reader through the journey of the development of the right to privacy. Through a comparative analysis of data protection standards, the author attempts to establish an international benchmark for personal data rights, and assesses the Indian position in relation to this benchmark.

Agrochemicals and *Data Exclusivity* seeks to study data exclusivity with reference to current interpretations of Article 39 of TRIPS. Here, much of the focus is on data exclusivity in the field of agrochemicals against the backdrop of the development of intellectual property rights in India.

In *Adjudicating Data Protection cases through WTO,* inspired by the alleged acts of economic cyber espionage between China and USA, the author delves into the possibility of litigating commercial

cyber espionage claims through the WTO Dispute Settlement Body (DSB) as a TRIPS violation and as a non-violation claim. The possibility of unilateral trade sanctions as a countermeasure is also analysed.

In *Remembering to Forget: A Legislative Comment on the Right to Forget in The Data (Privacy and Protection) Bill, 2017*, the author provides a comprehensive analysis of the recently proposed privacy bill with special emphasis on the right to be forgotten.

Also delving into the right to be forgotten is a special article, *Privacy Law: Right to be forgotten in India*, in which the author seeks to analyse the regulations surrounding this right in India with reference to various EU directives and the recently introduced General Data Protection Regulation (GDPR). The article also seeks to draw attention to the dilemma of data retention and deletion measures in a world of automated machine learning.

The Law Review Team hopes that the present volume proves to be an insightful read for all its readers and that the collection of articles on this topic is both unique and appreciable. We hope the readers have as much fun reading it as we did putting it together. We welcome any feedback to improve the quality of our journal and would like to thank all the individuals that encouraged and supported us in the publication of this volume.

Editorial Board

BLESSING NOTE FROM HON'BLE JUSTICE A.K. SIKRI

Justice A. K. Sikri
Judge
Supreme Court of India

Tel.: 23016022
23016044

September 18, 2018

MESSAGE

From a perusal of the past editions of this publication, it is clear that this journal works towards highlighting crucial legal developments at both the international and the national level. By analyzing these issues from the perspectives of the various stakeholders, the journal provides a perfect springboard for further debate and discussion.

This issue of the NLIU Law Review is special in that it focuses on a specific theme: *Data Protection and Privacy*. Not only is this a topic of contemporary relevance but one requiring much clarification and engagement. The articles put forward in the pages to follow tackle some of the issues falling within this theme and arrests the reader with their quality and depth of research.

This issue and its contents are promising signs for the future of the legal profession and I applaud the authors for their work. I would also like to extend my blessings and support to the faculty and students of the NLIU Law Review. May this be the first of many 'special' issues and may this journal continue to be a vibrant and stimulating source of learning and discussion.

(A.K. Sikri)

2, Moti Lal Nehru Marg, New Delhi-110011

PRIVACY LAW: RIGHT TO BE FORGOTTEN IN INDIA

*Prashant Mali**

I. INTRODUCTION

The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence; the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them. Therefore, the right to be forgotten is based on the autonomy of an individual becoming a right holder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests.

The right to be forgotten was recognized for the first time in India through the judgment delivered by Karnataka High Court in the matter of *Sri Vasunathan vs The Registrar-General* in 2017. A decade ago, however, a similar term, namely the "right to forget," was already a topic of debate. But viewed precisely, the active and the passive side of the "forget" medal are not identical, and the right to be forgotten should not be confused with the right to forget as happens frequently in blog discussions.

Basically, "Right to be forgotten" or "Right to be Erased" provides a right to individual to request for removal of his/her personal data floating around through Internet. The simple rule behind data erasure is that whoever is using the data has volunteer consent from the data owner. So, when the consent is withdrawn, the owner has a right to

have his data erased.[1] Also when the data controller has no legal right to process the data, the data should be erased.[2] In case of data erasure, whoever has the data access or whoever is processing the data has to erase it and have to remove any links, copies or replication of data. The origin of this right is traced from French jurisprudence on the "right to oblivion"; which was to make social integration easy for offenders who had served their sentence on basis of the publication of information of their crime.[3] Based on French jurisprudence, European Union Data Protection Directive, 1995 acknowledged the right to be forgotten, by introducing Article 12, which specifies that the member state should provide people to control, ratify, erase or block data related to them.

The significant technical challenge for implementation of "Right to be forgotten" is defining "personal data". According to Article 17 of European Union (EU) Directives, the term "personal data" means *any information relating to the individual*. Such a definition raises ambiguities on issues like collective information - information which may not identify any person individually but pointed towards the family. The identification of personal data becomes more complicated when it comes to erasure of derived data about individuals used in statistics or in another form of aggregated information. Once, there are reasonable grounds for data erasure, it is not clear practically how this erasure will be enforceable. According to EU, every individual has a right to control his or her private data, especially if they are not public figures.[4]

---

*Prashant Mali is the president and founder of Cyber Law Consulting (Advocates & Attorneys), Mumbai. The author may be reached at cyberlawconsulting@gmail.com.

[1]General Data Protection Regulation (EU) No. 2016/679 of 27 April 2016, Right to erasure, art. 17, 19, (hereinafter "GDPR").

[2]*Id*. art. 18, 19.

[3]Loc.gov. *Online Privacy Law: France, Law* Library of Congress (2018). https://www.loc.gov/law/help/online-privacy-law/france.php.

[4]*Supra* note 1, art. 18,19.

II. RIGHT TO BE FORGOTTEN UNDER EU DIRECTIVES

To make "*right to be forgotten*" enforceable EU introduced (Directive 95/46/EC) in 1995. In the EU in particular, this "*right to be forgotten*," was gaining increasing traction as a potential foundation of privacy regulation (Bennett, 2012). According to Vice President of the European Commission, Vivean Reding, the EU data protection reform, which was well overdue, should include provision for removal of online personal information.[5] In 2014, the Court of Justice of the European Union (CJEU) established the 'Right to be Forgotten' and accordingly, "*Every individual has the right – under certain conditions – to ask search engines to remove links with personal information about them.*"[6] As of March 2017, Europeans had submitted over 715,000 requests to deactivate two million URLs. Google has deleted over forty-three percent of those, approximately 732,000 links.[7] In fact, according to EU regulations, social media networks also need to erase personal data of individuals when asking under laws allowing people the "*Right to be Forgotten*".[8] At the same time, the Court's decision has stirred debates focused on the tension the decision raised between a person's right to privacy and freedom of

[5]Viviane Reding, Vice President, (EU), *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF.

[6]HUFFPOST, *Do we Have a Right to be Forgotten?* https://www.huffingtonpost.com/lindsay-hoffman/do-we-have-a-right-to-be_b_7812564.html [last visited Feb. 26, 2018].

[7]Weaver, M., *Google 'learning as we go' in row over right to be forgotten*. THE GUARDIAN. https://www.theguardian.com/technology/2014/jul/04/google-learning-right-to-be-forgotten [last visited 26 Feb. 2018].

[8]Catherin Stupp, *Germany set to fine social media platforms millions over hate speech*, EURACTIV, https://www.euractiv.com/section/digital/news/germany-plans-to-fine-social-media-platforms-millions-over-hate-speech/.

expression. The CJEU offered little guidance in determining when personal information is subject to mandatory erasure due to irrelevance or inadequacy. The opinion on "right to be forgotten" differs immensely between America and EU countries. According to America, transparency, the right to freedom of speech and expression is a priority. The publication of truthful information about individual or corporation is favoured by America. But, the European court of justice legally freezes the "*Right to be Forgotten*" as a human right in the *Costeja* case[9] against Google.

In the year of 2010, Mr. Costeja file a complaint against Google and Spanish Newspaper at National Data Protection Authority of Spain. In his complain, he mentioned that when he searches his name on Google, the search results show a link of newspaper article about a property sale made by him to replay his personal debts.

The authority dismissed the complaint against newspaper as they had the legal obligation to publish the property sale information. But authority allowed the complaint against Google.

In this matter, Google argued that as no physical server in Spain held the data and data are processed outside the European Union, it does not come under European Data Protection Directives. As a matter of practice, when Google receives a takedown notice for linking to infringing content, it removes those links from all of its sites across the world, so could the same not be done for private information?[10]

[9]Google Spain SL &Anr. V. Agencia Española de Protección de Datos&Anr, ECLI:EU:C:2014:317**,** Grand Chamber, (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

[10]Manjoo, F., *Right to Be Forgotten' Online Could Spread*, NYTIMES. https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [last visited Feb. 24, 2018].

The Court of Justice of EU finally stated that: The search engine companies are controllers of their services[11] and whoever promote and market their services within EU, the Data Protection Directives ("DPD") applies to them and consumer have the right to request such search engine companies to remove links or information associated with him/her. After this again the matter comes back to The Court of Justice of EU for removing the links from global domains rather than geo-limiting delinking.[12] After this decision, other search engine companies like Bing have already begun implementing the decision in Europe.[13]

There is one more case of Europe against Facebook, which does not talk about "*right to be forgotten*" but it gives an approach for erasing data.[14] This case basically explains erasing data by not displaying it to anybody. In this case was filed by Max Schrems, who asked Facebook to provide him all his personal information had on him. Initially, he received PDF file more than 1000 pages. This file also includes information, which he thought was deleted. Therefore, he decided to file a complaint against Facebook Ireland in front of the Irish Data Protection Commissioner.

Initially, he had filed 22 complaints against Facebook, which includes subjects such as shadow profiling, excess personal data, not removing data, face recognition. Addition complaints were filed in the year of

[11]Supra Note 1, ⁋⁋ 32, 33, 34.

[12]*CNIL, Right to delisting: Google informal appeal rejected,* https://www.cnil.fr/en/right-delisting-google-informal-appeal-rejected-0 [last visited Feb. 27, 2018].

[13]*See*, for example, Luciano Floridi, *Right to be forgotten poses more questions than answers,* THE GUARDIAN, https://www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-more-questions-than-answers-google.

[14]The Data Protection Commissioner v. Facebook Ireland Limited &Anr., High Court Ireland, Oct. 3, 2017, http://www.europe-v-facebook.org/sh2/HCJ.pdf.

2011, which contains subjects such as: tracking user's location via like button, picture link deletion, frequently changing policies.

The main issue, in this case, was that the data i.e. posts, pock, chat messages, friends, were not deleted by Facebook even though he had clicked on the delete button. Instead of removing data from a server, Facebook had made data in "invisible" mode. Even images were not deleted, only links of the images were removed.

After a long legal battle, the procedure ended in 2014 with the decision by Max Schrems, to withdraw the 22 complaints made initially.

Following the withdrawal of the complaint, an Austrian style class action lawsuit was started against Facebook in August 2014 with the aim "to make Facebook finally operate lawfully in the area of data protection".[15] This complaint has mainly focus on following points:

1. The Data use policy of Facebook, which is not legally valid under EU law.
2. There is no effective consent to many types of data use.
3. Support of the NSA's 'PRISM' surveillance programme.[16]
4. Tracking Internet user's actions on external websites.
5. Monitoring and analyzing users through "Big data techniques".
6. Unlawful introduction of 'Graph Search'
7. Unauthorized transfer of user data to external applications.

[15]EUROPE-V-FACEBOOK, http://europe-v-facebook.org/EN/Complaints/Class_Action/class_action.html [last visited Feb. 23, 2018].

[16]Top secret program allowing the NSA access to data from Google, Facebook, Apple and other major IT-companies.

On 1st of July 2015, The Court of Vienna rejected the case on procedural grounds, because Max Schrems used Facebook account for commercial promotions of his publications. The case transfers the case to a higher tribunal, and Max Schrems said he wants to appeal the decision. This suit is still under procedure at Austrian Supreme Court, so the clear conclusion is yet to be declared.

Analysis: In Facebook case, the interesting part is, Facebook has shown two different approaches to erase data from public domain: 1) Making Data invisible, 2) deleting only links to a file. Facebook just remove the links or make data invisible to user who wants to delete it. The same logic applies to everyone who was accessing or had permission to access such data. For example, if the user's profile is a public profile then people from public domain has access to profile or if the profile is private then his friends can access such profile. Once the user erases the data, Facebook still has the access to the data, as the data is not originally deleted from the Facebook database. Thus, if think from the perspective of the users who had access to the data before deletion, the data is deleted. But, the data is only removed from access domain.

Thus, removing links to the files or making data status invisible can deny the access to data. This approach is similar to the Google Case. But in case of Facebook no one can access erased data by using different permutations. Google actually removed the data access from the specific environment rather than deleting it from the public domain. Making data invisible works for the environment, which has control over access to data. In case of Google, it does not have any control over who has access to the data. Whereas, Facebook has a specific environment, which has control over who has access to data.

III. RIGHT TO BE FORGOTTEN WITH RESPECT TO DATA RETENTION & GDPR

As pointed out by Korenhof et al. (2014) the timing of data retention plays a part in this debate as longer periods of data retention make it difficult for digitally recorded actions to be forgotten. Privacy laws encompass any policy or legislation that governs the use and storage of personal information about individuals whether by the government, public, or private entities. As Hetcher (2001) points out, the Internet can often lead to a "threat to personal privacy" due to the "ever-expanding flow of personal data online." This notion of privacy and security of personal data has become one of the more significant public policy concerns generated by the Internet, leading to "legal and regulatory challenges" (Salbu, 1998).

To unify data protection for all within the European Union, GDPR was introduced on 27th April 2016. The GDPR will be applicable in European Countries form 25th May 2018. The aim of introducing GDPR is to give control of personal data to the citizens and to simplify data erasure process and regulatory environment for international business. According to Article 17 of GDPR, *the right to be forgotten* means:

- Data Subjects have the right to obtain erasure from the data controller, **without undue delay**, if one of the following applies:

    1. The controller doesn't need the data anymore

    2. The subject withdraws consent for the processing with which they previously agreed to (and the controller doesn't need to legally keep it [N.B. Many will, e.g. banks, for 7 years.])

    3. The subject uses their right to object (Article 21) to the data processing

4. The controller and/or its processor is processing the data unlawfully

5. There is a legal requirement for the data to be erased

6. The data subject was a child at the time of collection (See Article 8 for more details on a child's ability to consent)

- If a controller makes the data public, then they are obligated to take reasonable steps to get other processors to erase the data, e.g. A website publishes an untrue story on an individual, and later is required to erase it, and also must request other websites erase their copy of the story.

Exceptions to above provision:

The Data might not be erased if any of the following applies:

- For exercising the right of freedom of expression and information;

- For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- For reasons of public interest in the area of public health

- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

- For the establishment, exercise or defence of legal claims.

More generally, the length of data retention has become an issue in this debate over privacy. The question is whether the benefits of privacy (less data retention) for consumers outweigh any potential costs to consumers (lower quality search results). The right to erasure does not provide absolute "*right to be forgotten*". Every individual has a right to erase personal data and prevent processing of data save for but in certain circumstances.[17] European filtering of Internet content worldwide through the right to be forgotten effectuates international censorship in the guise of privacy. As per Article 17, GDPR has a data retention provision when it requires. For example, GDPR has provision for employee data retentions. GDPR contains provisions for in what circumstances, which personal data should be retained and for what time period.

Before GDPR, UK already has their data protection regulations. Similar to UK regulations GDPR has introduce some regulation in terms of employee data retentions which are as below[18]:

- The right to be informed: "The employer obelized to inform employee about how personal data will be used"
- The right to ratification: inaccurate or incomplete data needs to be rectified.
- The right to be forgotten: No longer required data needs to be deleted from employer's database.
- The right to block or suppress from processing: The employee should have right to block or suppress from processing his/her personal data.
- The right to data portability: Employee should have right to reuse his/her personal data for personal purpose during certain circumstances.

[17]According to Dr. Guy Bunker, SVP Products at Clearswift (Data Security Company)

[18]As defined in article by Ronan Daly Jermyn, A leading law firm in Chambers of Europe.

To implement right to erasure properly, every organization needs to implement an accurate mechanism to erase data absolutely from their system on demand by their customers or clients meaning that the data should not exist in backups as well. [19] According to GDPR, if you are using a third-party service for data storage then also, the organization needs to be aware of what is the mechanism third party is using at the time of data erasure. If the third party does any mistake in data erasure then also the organization will also be jointly liable for such mistake. The GDPR will not only apply to employers processing the personal data of their employees, but also to HR service providers that process such data on behalf of the employer ("data processors"). [20]

Articles 17 (2) and 18 (1a) mandate that data processing after retention period is also not permissible, meaning that once the data has to be deleted then data controller cannot use such data for other purposes.

One challenge faced by the Indian legal system is that currently, most privacy laws at the federal level predate the technologies, such as the Internet, that raise privacy issues. In recent years, innovations such as behavioral advertising, location-based services, social media, mobile apps, and mobile payments lead to heated debates over an individual's privacy and security. Given that most innovations and regulations occur in the EU, we study here the effects of changes in those policies abroad and their implications for the India Internet.

[19]D. Froud, *GDPR: Does the Right to Erasure Include Backups? - Froud on Fraud*, FROUD ON FRAUD. http://www.davidfroud.com/does-right-to-erasure-include-backups/.

[20]AMCHAM.BE, *The new EU data protection regime from an HR perspective*. http://www.amcham.be/publications/amcham-connect/2016/march/fieldfisher-gdpr-data-protection-human-resources-hr-perspective.

IV. EFFECT OF RIGHT TO BE FORGOTTEN ON MACHINE LEARNING

In machine learning regarding the deletion of privacy data, the right to be forgotten is the right to support one's informational autonomy by giving the decisive power to data providers. The management of private data and handling of deletion requests of such data are the challenges facing machine learning. Now, removing personal information from prominent search engines like Google challenges fundamental aspects of machine learning. One major question is what will be the effect of data removal on knowledge base machine learning algorithm. As per the previous approach continuously increasing the amount of information will enhance the performance of the result.[21] So, deletion of information from existence will reduce the quality of results even more. So, to avoid this drawback machine learning algorithm should be made more powerful which can make information more generalized in analytical results. To implement this idea, organizations need to use the approach of encoding sensitive data with some privacy protection means and then analysed by machine learning algorithm and then only the information should available for inspection.[22]

Now, one interesting fact about the Mr. Costeja's case is that the original information about Mr. Costeja is never removed from the database. At present, one can still find an online version of the newspaper. So, what machine learning does is once the app done with the data object and memory is freed or erased, the data does not disappear immediately. The chunk of memory is put into a linked list and then it will be processed and then make a software memory part

[21]B. Malle, P. Kieseberg, E. Weippl, A. Holzinger: *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*, Workshop on Privacy Aware Machine Learning (PAML), August 2016.

[22]Green, A. and Green, A., *The Right to Be Forgotten and AI*. VARONIS BLOG. https://blog.varonis.com/right-forgotten-ai/ [last visited Feb 23, 2018].

available for re-use. So, at a certain point of time data does not dispose of instantly. Now machine learning works with a large number of data, due to which the software continuously allocating and deleting data, sometimes data might be present in disposal queue.

As per GDPR, if it is necessary to remove personal information on request, one cannot defend on technical complexity. So, there needs to be some technical solution to make data completely invisible. So the now machine learning algorithm should be based on any anonymity technique or pseudonymization to avoid storing identifiable data, to implement right to be forgotten.[23] According to the technology experts, to make data unavailable form the public domain, there are four factors, which need to be taken into consideration: 1) Time[24] 2) Meaning of Information 3) Regularity 4) Space. To identify or to make a decision which data needs to be deleted when *right to be forgotten*' accessed by any person the above four factors needs to be analysed for data erase.

V. RIGHT TO BE FORGOTTEN IN INDIA

However, In India there are no specific data protection laws, so ad-hoc judicial attention of the court is sought. In the writ petition *Sri Vasunathan v The Registrar-General*[25] before the Karnataka High Court, the Court observed that "*This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases*

[23]Malle, B, Kieseberg, P, Weippl, E & Holzinger, A 2016, *The right to be forgotten: Towards Machine Learning on perturbed knowledge bases*, 251-266, Springer Lecture Notes in Computer Science LNCS 9817. Springer International, Privacy Aware Machine Learning (PAML) for health data science, Salzburg, Austria.

[24]*See* Sartor, G. *Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data* (2018).

[25]Sri Vasunathan v. The Registrar General & Ors., http://www.iltb.net/2017/02/karnataka-hc-on-the-right-to-be-forgotten/

involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned." Hence, the Court directed its registry that petitioner's daughter's name should not reflect in the case-title of the order or in the body or the order in the criminal petition. The woman's father had approached the high court for seeking the directions to remove woman's name from the earlier order passed by the high court. The petitioner had stated that his daughter's relationship with her husband and her reputation in society will get affected if her name remains associated with her earlier case.

Similarly, Once Justice Sanjay Kishan Kaul delivered his opinion on right to forgotten and he stated, "The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet" [26]

In contrast with above-mentioned opinion, Gujarat High Court *Dharamraj Dave v. State of Gujarat*[27]) pointed out that there is no attracted law to remove judgment from Google search or Indian Kanoon and petitioner does not have sufficient arguments to prove "uploading judgment on the Internet is a violation of Article 21 of the Constitution." These cases demonstrate the lack of legal framework and the inability of the judiciary in interpreting the right to be forgotten. So, India requires specific Data protection Laws to protect right to be forgotten.

In 2017, in Justice K S Puttaswamy's case, the "*right to be forgotten*" defined by The European Union Regulations, 2016, has been recognized. The following are the considerations made by the Supreme Court:

[26]Justice K. S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1.
[27]Dharmraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019.

1. Children around the world have access to the digital media. They are constantly making their footprints on social media networking. They are passing the data with chat, Bluetooth, web downloading, Emails, Facebook, Google, Hotmail, and Instagram. They should not be affected by their childish mistake or naivety, their entire life. So, the parents of such children or the person can request for remove data or personal information regarding their childhood or their children.[28].

2. People change and every individual should be able to move forward in life and should not be stuck by the mistake done in past. 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 view expressed by them will stay forever with them.

3. Whereas this right to control the dissemination of personal information does not amount to total erasure history, as this right is a part of right to privacy and should be balanced against other fundamental rights like right to freedom of expression, or freedom of media.

4. Thus, Right to be forgotten means, when the data of any person is no longer required or who expects that his/her personal data will be no longer stored or processed then he/she should be able to remove it from the system where the information is no longer necessary, relevant or is incorrect or is illegitimate. But, Right to be forgotten does not mean to remove data or personal information, which is necessary for exercising right of freedom of expression and information,

[28]Michael L. Rustad, SannaKulevska, *Reconceptualizing the right to be forgotten to enable transatlantic data flow*, 28 HARV. J.L. & TECH. 349.

> for the performance of the task carried out in public interest, in public interest in the area of public health, scientific or historical research purpose, exercise or defense for legal claim.[29]

As a part of privacy, every individual should be able to control his/her personal data and to be able to control his/her life encompasses his right to control his/her existence on the Internet. But this does not mean that a criminal can obliterate his past, but there are various degrees of mistake, small or big, it cannot be said that a person should be profiled to the extent many times more than his mistake.

After the *Justice K.S Puttaswamy* judgment, Government of India decided to constitute a committee of Experts to regime Data Protection Laws in India. So, under the chairmanship of former Supreme Court Justice Shri B N Srikrishna a committee has released a white paper on Data Protection Framework for India on November 27, 2017.[30]

According to the white paper, the consent should be one of the grounds for data processing. But, here the consent should be valid. As the committee noticed that one of the three Internet users across the world is the child under the age of 18. So, a data protection law must be efficient to protect their interests, while considering their vulnerability and exposure to risks online.

The committee has also commented on Purpose of Data Collection. According to White Paper, there should be some specific purpose for personal data collection. Also, the collected personal data should be erased once the purpose is fulfilled. The committee also mentioned in

[29]Justice K S Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1, ¶ 69.

[30]*White paper of the Committee of Experts on a Data Protection Framework for India*, Government of India, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final _v2.1.pdf.

the report that, the person should have a right to confirm, access, and rectify his or her own data.

Also, the white paper talks about the issues with right to be forgotten provisions under data protection law. Accordingly the right to be forgotten should not conflict with freedom of speech and expression and while formulating a right to be forgotten, it is necessary to identify the third party can be held liable for failing to comply with erasure request or not.

VI. CONCLUSION

"Right to be forgotten" is becoming very important for the legal aspect as well as technical aspect. Due to technical complications, legal provisions for such right are also getting complexes. Now as "Right to be Forgotten" is increasingly being viewed as a part of the right to privacy. When we talk about "Right to be forgotten", the information will be considered true so the right to free expression and publication could not be overshadowed by "Right to be Forgotten".[31] In India, this debate is still continuing as India does not has any specific provision for providing such a "Right to be forgotten". India is still dependent on ad-hoc jurisprudence to access this right. As the Union Government of India is making laws for Data Protection and the Committee has recognized this right in Chapter 10 of White paper, it is expected that there will be provision for such a right in the upcoming law on data protection.

[31]Justice K. S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1, ¶ 68.

PERSONAL DATA EXCHANGES – TOWARDS AN EQUITABLE FOURTH INDUSTRIAL REVOLUTION

*Narayani Anand**

Abstract

This paper aims to examine the effectiveness of the newly adopted Regulation (EU) 2016/679 – popularly known as the General Data Protection Regulation (GDPR) – in protecting data privacy, and analyses the extent to which it prioritises individual interests over those of data aggregators. Three key aspects of data protection, viz. 'notice & consent', 'opting-out' and 'anonymisation & pseudonymisation' have been selected for this analysis. Their presence has then been traced in the GDPR, and compared with the older data protection law in Europe – Directive 95/46/EC, also known as the Data Protection Directive of 1995. Finally, a consumer-centric system of data exchange and management has been proposed vis-à-vis the existing provider-centric model, in the form of a Personal Data Exchange – modelled upon considerations emerging from three separate research approaches – 'Primary Market', 'User Privacy Risk Attitudes' and the 'Personal Information Management System'. This has been proposed as an end towards which the three aspects of

data protection in the GDPR discussed above could be developed.

I. INTRODUCTION

In the age of the internet, what once seemed to be ideas of fiction straight out of Isaac Asimov's works have transformed into reality. The interaction of the internet with common technologies has resulted in outcomes that are altering the way we live. The Executive Chairman of the World Economic Forum (WEF) describes the dawn of this age in words that spell no less than a thrilling anticipation: "we stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before."[1]

A transformation "unlike anything humankind has experienced before" will create equivalent challenges. The technical and regulatory frameworks to sustain the Fourth Industrial Revolution are undergoing fundamental changes.

The recently adopted General Data Protection Regulation (GDPR) of the European Union (EU) is being touted as the "world's toughest

*Narayani Anand is a third year law student at Campus Law Centre, Faculty of Law, University of Delhi. The author may be reached at narayani.anand93@gmail.com.

[1]Klaus Schwab, *The Fourth Industrial Revolution: What it Means, How to Respond*, WORLD ECONOMIC FORUM (Jan. 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

privacy law".[2] It bolsters the existing provisions for data protection in the EU and is set to harmonize the regulatory framework of its member countries by enacting binding laws.

II. THE EMERGENCE OF BIG DATA

The Fourth Industrial Revolution represents a fundamental change in the way we live, work and relate to one another. It is a new chapter in human development, enabled by extraordinary technology advances commensurate with those of the first, second and third industrial revolutions.[3] We are living on the cusp of opportunity and calamity. The Fourth Industrial Revolution promises technological advancements that can dramatically transform the nature of life on Earth at an unprecedented pace.[4]

This industrial revolution will bring together digital, physical and biological systems. While its conception might still seem abstract, it will be characterised by technologies that will metamorphose the way we live and interact with the physical world. An example of this is the proliferation of artificial intelligence in manufacturing and service delivery.

The key to conceptualizing any of these breakthrough technologies lies in a fascinating concept that is fast taking over the digital world: 'Big Data.' Big Data' is a term that has produced definitional challenges for the sheer variety of contexts it can be understood in. A

[2]David Meyer, *Here Come the World's Toughest Privacy Laws*, FORTUNE TECH (Apr. 14, 2016), http://fortune.com/2016/04/14/eu-parliament-gdpr/.
[3]World Economic Forum, *The Fourth Industrial Revolution*, WORLD ECONOMIC FORUM (June 11, 2018), https://www.weforum.org/focus/fourth-industrial-revolution.
[4]HeeradSabeti, *The Fourth Sector Is a Chance to Build a New Economic Model for the Benefit of All*, WORLD ECONOMIC FORUM (Sept. 08, 2017), https://www.weforum.org/agenda/2017/09/fourth-sector-chance-to-build-new-economic-model.

definition appearing in a NASA paper, for example, has been argued to be relative and ambiguous[5] for its use of the terms "large" and "more resources" to define, respectively, the size of the data sets and the storage required to fit this data. Further, in a McKinsey study[6] that defines big data as "datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze", researchers have acknowledged that "this definition is intentionally subjective and incorporates a moving definition of how big a dataset needs to be in order to be considered big data."

In order to use the most suitable definition for our purpose, it is necessary to emphasize on the regulatory challenges that result from the management of big data. Big Data, therefore, refers to "data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges."[7]

Possibly the first use of the term 'big data' can be traced to the year 1989, when best-selling author Erik Larson penned an article for Harpers Magazine speculating on the origin of the junk mail he received. He wrote that "the keepers of big data say they are doing it for the consumer's benefit. But data have a way of being used for purposes other originally intended."[8] In 1999, the term Big Data

[5]Gil Press, *12 Big Data Definitions: What's Yours?,* WORLD ECONOMIC FORUM (Sept. 3, 2014), https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#1cd6022413ae.

[6]James Manyika et al., *Big data: The Next Frontier for Innovation, Competition, and Productivity,* MCKINSEY & COMPANY: DIGITAL MCKINSEY (May, 2011), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

[7]The OXFORD ENGLISH DICTIONARY (2013 ed.), http://www.oed.com/view/Entry/18833#eid301162178.

[8] Bernard Marr, *A Brief History of Big Data Everyone Should Read*, WORLD ECONOMIC FORUM (Feb. 25, 2015), https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/.

appeared in research published by the Association for Computing Machinery. One of the aspects that was lamented was the propensity for storing large amounts of data with no way of adequately analysing it. When seen with an undiscerning eye – random sets of data on an individual's social media activity would seem useless. Enterprises, however, are using this data to strike gold, through what is known as data analytics. Data analytics examines large amounts of data to uncover hidden patterns, correlations and other insights, helping organisations harness their data and use it to identify new opportunities. That, in turn, leads to smarter business moves, more efficient operations and higher profits.[9] The difference between enterprises of yesteryears and today is that the latter have understood the importance of capturing all of the data flowing into their businesses and using analytics to extract its maximum value. The Internet of Things (IoT), explained as the concept of "connecting any device with an on and off switch to the Internet and/or to each other",[10] has made it possible to collect and transmit data – in real time. In the past, businesses would collect only a limited type and quantity of data – to be used in making future decisions. This simultaneous collection, transmission and analysis are revolutionizing the way in which enterprises interact with us – the consumers. They now operate faster and stay responsive and are gaining a superior competitive edge.

Consider the case of Aptude,[11] an American IT development firm that uses big data technologies like Hadoop to help its clients harness maximum value through data analytics.

[9]SAS, *Big Data Analytics – What it is and Why it Matters*, SAS INSIGHTS (June 12, 2018), https://www.sas.com/en_us/insights/analytics/big-data-analytics.html.
[10]Jacob Morgan, *A Simple Explanation Of 'The Internet Of Things'*, FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#416754321d09.
[11]Aptude, *Big Data Case Study – Hadoop Implementation*, APTUDE (June 12, 2018), https://www.aptude.com/about/case-studies/big-data-case-study-hadoop.

Hadoop is an open-source software framework for storing data and running applications on clusters of commodity hardware. It provides massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks or jobs.[12]

One of Aptude's clients, a leader in the Transportation and Logistics domain, had their trucks travelling roughly 8 million miles per day. The client needed a method to effectively analyse truck travel patterns to gain an understanding on a myriad of issues including how many "empty miles" were accrued on routes and subsequently make adjustments for more efficient deliveries. Utilising their in-house logistics tracking software, the client had been temporarily storing log files. Due to the massive amount of data being pushed into these files, they were only retaining this data for a short duration. Additionally, since the data was unstructured, developers would have to manually extract, parse, and search the data every time they needed to perform an analysis.

A solution was needed to add structure to these data logs, provide the ability to run ad-hoc queries when issues occurred and perform analytics against the data to improve trucking route efficiency.

After obtaining information through their discovery and requirements gathering process, Aptude architected a big data solution utilising Hadoop in conjunction with a combination of other key open-source components to harness its full potential.

With minimal hardware resources and a collection of open-source software requiring no licensing fees, Aptude realised the Client's big data solution at a fraction of the cost a traditional database solution

[12]SAS, *Hadoop – What is it and Why Does it Matter?*, SAS INSIGHTS (June 12, 2018), https://www.sas.com/en_in/insights/big-data/hadoop.html.

would have required. The Hadoop implementation resulted in cost and time savings, with an additional benefit from the boost in productivity they will achieve with their new analytical assets.

Three key uses of big data analytics to businesses have been identified as:[13]

1. Cost reduction

Cloud based analytics and big data technologies like Hadoop provide notable cost advantages when storing huge amounts of data, as well as in identifying better ways of doing business.

2. Time reduction

In-memory analytics and the processing speeds of Hadoop, along with the ability to analyze new forms of data, enables businesses to analyze information on an immediate basis and make faster decisions.

3. New products and services

Businesses now have the power to tailor their products to fit the customers' needs and preferences One of the most ambitious things an organization can do with big data is to employ it in developing new product and service offerings based on data.

With the multifarious uses of big data- it is evident that its role has expanded significantly.

While in 2013 the IoT market in manufacturing operations was already worth $42.4 billion, it will grow to $98.9 billion by 2018. As with mobile technology 15 to 20 years ago, the IoT revolution is just

[13]Davenport &Dyché, *supra* note 3.

beginning, and over the next two decades it will have a profound impact on businesses, the economy and society.[14]

From the 13 industries that were studied in a research conducted by Tata Consultancy Services(TCS), nearly 79% of the companies used the IoT to track their customers, products, the premises in which they do business with customers, or their supply chains. Perhaps the most significant was the average revenue increase in areas of business where IoT initiatives were deployed – a strong 16% in 2014. In addition, about 9% of firms had an average revenue increase of more than 60%.[15] The CEO of TCS has said that it is because of these developments that he believes data is the new currency.[16]

The value creation offered by big data has become an inevitable asset for companies who want to compete seriously. Research has revealed that a retailer embracing big data has the potential to increase its operating margin by 60 per cent. It also predicts the leveraging of data-driven strategies by, both – established competitors and new entrants – to compete, innovate and capture value.[17]

Data is now part of every sector and function of the global economy and, as an essential factor of production, much of modern economic activity simply could not take place without them.[18]

[14]Natarajan Chandrasekaran, *Is Data the New Currency*?, WORLD ECONOMIC FORUM (Aug. 14, 2015), https://www.weforum.org/agenda/2015/08/is-data-the-new-currency/.
[15]Tata Consultancy Services, *supra* note10. http://sites.tcs.com/internet-of-things/wp-content/uploads/Internet-of-Things-The-Complete-Reimaginative-Force.pdf.
[16]*Id.*
[17]Michael Chui et al., *Big Data's Potential for Businesses*, MCKINSEY & COMPANY (May 13, 2011), https://www.mckinsey.com/mgi/overview/in-the-news/big-data-potential-for-businesses.
[18]*Id*.

III. DATA PROTECTION AND PRIVACY

A. The Need for Data Protection

The data collection activities of businesses have highlighted the pressing need for strong data protection laws. 'Data protection' is defined as the 'legal control over access to and use of data stored in computers.'[19] It is the law designed to protect personal information, which is collected, processed and stored by automated means or intended to be part of a filing system.[20]

Once the data in paper files is converted into a language and format readable by electronic devices, the extraction of personal data from one record and its correlation with the same personal data in another file becomes an easy and inexpensive task. The end-result is a combination that can create a 360 degree online-identity of a person, signalling alarm bells for an individual's privacy.

Consider, for example, the Yahoo! data breach in September 2016. The once dominant Internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by "a state-sponsored actor," in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm. The breaches knocked an estimated $350 million off Yahoo's sale price.[21]

B. Data Protection In The European Union

[19]THE OXFORD ENGLISH DICTIONARY (2013 ed.) http://en.exforddictionaries.com/definition/data_protection.
[20]Privacy International.
[21]Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

The strongest and most comprehensive laws are in the countries of the European Union (EU) and European Economic Area that have implemented the 1995 Data Protection Directive. Following the common directive for the region, EU member countries had enacted individual data protection legislations within their national jurisdictions.

After four years of negotiations and formalities, in April 2016, the EU Parliament adopted the "world's toughest privacy law";[22] the General Data Protection Regulation (GDPR). The GDPR will be enforceable from 25 May, 2018, after providing member states with a two-year transition period. Unlike the 1995 Directive that required member countries to pass enabling legislation, the GDPR will be directly applicable and binding on national governments. This will lead to harmonization and better clarity in implementation.

For the purpose of this paper, three aspects of data protection have been briefly examined and their presence has been located in the proposed GDPR. The aspects, viz., 'notice and consent', 'opting out' and 'pseudonymisation and anonymisation' have been chosen for their specific importance to data protection. Their effectiveness as standalone measures in the GDPR has been evaluated.

a) Notice and consent

In the 'Terms of Privacy' laid out by businesses for use of their services, 'notice' implies an informational declaration on the part of the company as to their data collection and processing activities. This may also extend to the notice for third-party data sharing. By clicking 'I agree' on to these privacy agreements, a user, at least theoretically,

[22] *Id.*

consents to the use of their data by the company in the manner so described in their agreement.

The 1995 Directive defined 'consent' in Article 2(h), as "[a]ny freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Article 7(a) required that Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent.

The GDPR has significantly increased the requirements for availing the user's consent, as well as extended to them more rights. Article 7 of the GDPR describes stringent 'conditions for consent' that mandate the controller[23] to be able to demonstrate that the data subject has consented to processing[24] of their personal data. It also requires that the manner for presenting the request for consent be easily distinguishable in an easily understandable form. Further, it provides for the right of the data subject[25] to withdraw such consent, as freely and easily as they give it.

However, aside from this, the GDPR also prescribes the situations in which processing shall be lawful.

Article 6(1) states that processing shall be lawful only if and to the extent that *at least one* of the following conditions apply:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

[23]General Data Protection Regulation (EU) No. 2016/679 of 27 April 2016, art. 4 §§ 33, cl. 7.
[24]*Id*., art. 4 §§ 33, cl. 2.
[25]*Id*. art. 4 §§ 33, cl. 1.

(c) compliance with a legal obligation to which the controller is subject;

(d) for protecting the vital interests of the data subject or of another natural person;

(e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and

(f) for legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Although other provisions in the GDPR are in-built to check the misuse of provisions under Article 6 (such as Recital 32, for example, which provides for the specific acts that constitute consent), the very fact of legalising the processing of personal data in situations besides where such consent is expressly provided, takes away from the primacy of individual consent. This effectively renders the 'consent' clause purely optional for data processing to be lawful, hence negatively impacting individual autonomy. It lends legal backing to the argument most commonly presented by businesses that the consent of users is secondary insofar as data collection and analytics is concerned. This means that organisations can cite "legal obligations" or "contractual performance", for example, and get away with processing a user's data, without their consent. Even with respect to specific conditions such as "legal obligation" under Article 6(1)(c) the recitals make it clear that the relevant "legal obligation" need not be statutory (i.e. common law would be sufficient, if this meets the

"clear and precise" test[26]). A legal obligation could cover several processing operations carried out by the controller so that it may not be necessary to identify a specific legal obligation for each individual processing activity.[27]

b) Opting-Out

'Opting-out' refers to the process of expressly deciding against the collection of information through cookies and sharing of usage and browsing data with third-parties. On websites, pre-ticked boxes that convey the user's consent for information sharing and receiving third-party promotions are the default opt-in options.

Under the 1995 Directive, controllers could rely on "opt-out" and implicit consent in certain situations.[28] The GDPR, however, requires "a statement or a clear affirmative action"[29] by the data subject to signal agreement

Recital 32 of the GDPR states that:

> *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly*

[26]*Id*., Recital 41 §§ 8.
[27]Bird & Bird, *Lawfulness of Processing and Further Processing*, BIRD & BIRD (June 12, 2018), https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/22--guide-to-the-gdpr--lawfulness-of-processing-and-further-processing.pdf?la=en.
[28]Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 3 – Consent*, IAPP (Jan. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/.
[29]*Supra* note 23, art. 4 §§ 34, cl. 11.

> *indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent."*

Therefore, the Regulation has created additional levels for consent over what was considered legitimate by the 1995 Directive. The latter required consent to be specific to the processing operations and the controller could not request open-ended or blanket consent to cover future processing. Significantly, while consent could be satisfied by an express statement, it also could be inferred from an action or inaction in circumstances where the action or inaction clearly signified consent. Hence, the Directive left open the possibility of "opt-out" consent.[30]

However, through Recital 32, the GDPR removes that possibility by requiring an unambiguous statement implying clear affirmative action on the part of the data subject.

As companies are finding new and improved ways to collect users' personal information and sell it to "third-parties" (most commonly advertisers and marketers), it is becoming increasingly difficult to 'opt-out' of information sharing. The option to limit the sharing of personal information by choosing "opt-out" is not immediately obvious on many websites and applications.

Data as a currency is being traded back and forth by companies to generate millions in profit. Opting out of data brokers and advertising

[30] *Id.*

schemes is notoriously difficult. Other sites make it so you have to provide more information about yourself in order to opt out.[31]

The new law safeguards against this to quite an extent – by mandating a positive "opt-in" mechanism rather than a negative "opt-out" mechanism that would imply consent. This should mean businesses giving special focus to making amply clear the data processing purposes for which consent would be sought.

However, Recital 50 of the GDPR provides for "compatible" operations, citing which consent for subsequent processing operations need not be obtained. These subsequent operations have to be compatible with those for which the data were initially collected. The laws of the EU or Member State may be used to determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

It also provides certain guidelines that the controller should take into account while determining compatibility, including "any link between those purposes and the purposes of the intended further processing; the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations."

While the above guidelines would serve as important safeguards against determining compatibility arbitrarily, Recital 50 provides wide grounds for organisations to manoeuvre outside the limits of consent.

[31]Dave Maass, *How Hard is it to Opt Out of Third Party Data Collection?*, ELECTRONIC FRONTIER FOUNDATION (May 21, 2013), https://www.eff.org/es/mention/how-hard-it-opt-out-third-party-data-collection.

Article 5 contains the principles relating to processing of personal data. Additional processing for reasons of "public interest, statistical purposes, scientific or historical research" will generally be considered compatible under Article 5(1)(b), and, would therefore, be an exception to the requirement for specific consent. Potentially, this exception is quite broad, as – wherever applicable – and read with Article 89 (which contains safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes), even withdrawal of consent by the data subject would not mandate the controller to rectify or erase the data. It would further impact the data subject's right to be notified of and object to processing operations, as well as restrictions on data portability and processing.

c) Anonymisation and Pseudonymisation

The Information Commissioner's Office (ICO) of the UK, an independent regulatory office which reports directly to the Parliament, defines 'anonymisation' as: "the process of turning data into a form which does not identify individuals and where identification is not likely to take place".[32]

Recital 26 of the GDPR defines anonymised data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable." The emphasis in this definition is on stripping the data of any identifiable information in a manner that makes it impossible to get insights on an individual even by the entity that carries out the anonymisation.

[32]Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice, Information Commissioner's Office*, INFORMATION COMMISSIONER'S OFFICE (June 12, 2018), https://ico.org.uk/media/1061/anonymisation-code.pdf.

There is an increasing reliance on anonymisation by organisations in order to broaden the scope of personal data use. Anonymisation of data is carried out to prevent the identification of individuals, organisations and businesses. It addresses ethical concerns regarding protection of people's identities for projects in research as well as for commercial and legal requirements. Common methods include hashing,generating a value or values from a string of text using a mathematical function[33] and encryption the process of using an algorithm to transform information to make it unreadable for unauthorized users.[34]

The Working Party, set up under The Article 29 of the 1995 Directive, had acknowledged that the principles of true data anonymisation were of a very high standard which data controllers often fell short of.

The 1995 Directive, in Rule 26 determining its application, laid down that:

> *"To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".*

The emphasis, thus, was upon identifiability of the data subject from all the means available for likely use by the controller or any other party. If no longer possible, identification would be ruled out and data would thus be considered anonymous while the data protection principles set out in the Directive would no longer apply.

[33]Techopedia,
[34]*Id.*

The GDPR continues this legacy by regarding anonymisation as the highest standard of data protection, thus excluding data that has been anonymised from its purview. Like its predecessor, the Regulation does not apply to anonymised data as defined in Recital 26.

The Regulation brings a novel concept to the data protection law in Europe, by introducing 'pseudonymisation' as a sort of middle-ground aimed at protecting individual privacy while at the same time allowing data controllers to utilise the data.

Article 4(5) of the GDPR defines 'pseudonymisation' as:

> *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*

There is more flexibility in the GDPR vis-à-vis the Directive, in terms of identifiability of individuals. The main point of difference between pseudonymised data and anonymised data is whether there can be re-identification with "reasonable effort".

Even though it falls within the Regulation, some provisions relating to pseudonymised data have been relaxed enough to allow data controllers to benefit from using the technique. Thus, controllers engaging in pseudononymisation of data will find it easier to use it for historical and scientific research purposes as well as in meeting the Regulation's security requirements.

Under the 1995 Directive, the Article 29 Working Party had observed the distinction between the two methods, by stating that "pseudonymisation is not a method of anonymisation" because re-identification remained a possibility, albeit a small one.[35] Therefore, even when the controllers deleted all identifying information on their end, the Directive would apply even if a third-party could reasonably identify the data in future.

In contrast, the GDPR is posed to provide more flexibility, by considering whether re-identification is "reasonably likely".

Pseudonymisation in its present form also facilitates the use and processing of data in excess of its original collection purpose.

Article 6(4) which determines use beyond original purpose for data collected without the data subject's consent, lists "the existence of appropriate safeguards, which may include encryption or pseudonymisation" as one of the factors to be taken into account while determining the compatibility (as discussed under (b.) above). Thus, the GDPR allows controllers who pseudonymise personal data more leeway to process the data for a different purpose than the one for which they were collected.[36]

Further, Article 11 says: "if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation. This Article also provides that the rights of the data subject contained in Articles 15 – 20, viz. right of access by data

[35]Data Protection Working Party Opinion 05/2014 on Anonymisation Techniques art. 29,

[36]Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 8 – Pseudonymization*, IAPP (Feb. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

subject, right to rectification, right to erasure (also known as the 'right to be forgotten') and so on, shall not apply where the controller is able to demonstrate that it is not in a position to identify the data subject. Certain valuable rights of data subjects with regard to control of their data under Articles 15-20 can therefore be waived off simply by the controller demonstrating that he can no longer identify the data subject through the available information.

In any case, the object behind data anonymisation is that the data subject should be nearly impossible to re-identify. The technique, however, falls short of practical and mathematical scrutiny.

It has been shown that 87% of the total population of the United States could be identified by only three markers – their 5-digit zip, gender and date of birth; even when typical data releases contain numerous other fields.[37] In effect, even though these would not be identifiable as standalone data points, storing them together would leave the data subjects susceptible to identification.[38] This, then produces a huge challenge for data controllers seeking to anonymise data.

De-identification – the primary process in anonymisation and pseudonymisation - fails to resist the inferring of sensitive information in boththeory and practice. Attempts to quantify the efficacy of de-intification techniques are unscientific and promote a false sense of security.[39]

In spite of ample scientific evidence to disprove the efficacy of anonymisation and pseudononymisation techniques in data protection,

[37]Sweeney, *supra* note 2.
[38]*Supra*
[39]Narayanan & Felten, *supra* note 1.

the GDPR has wholly excluded anonymised data from its purview, thus leaving millions of people vulnerable to re-identification. This poses an alarming risk to individual privacy, raising serious questions about the rationale behind this move. Further, the GDPR has constructed pseudonymisation regulations with some flexibility – allowing for data controllers to utilise data while also providing for some security measures. The existence of Article 6(4)(f) and Article 11 give great leeway for controllers to process data – a.) for additional purposes without the data subject's consent, and b.) having deleted the identifying information, by simply waiving key rights of the data subjects.

C. Finding A Middle Ground

On examining the efficacy of these three aspects of data protection and their treatment by the GDPR, it is observed that open data is given a preference over data privacy. This is seen, for example, where consent is only one among the six circumstances under which data processing would be deemed lawful[40] , and where – in case of additional processing operations – consent can be altogether done away with, by proving 'compatibility'.[41] Similarly, pseudonymisation has been constructed as a 'middle ground' between security and data use, allowing organisations much elbow-room for harvesting data.

Where "performance of a contract to which the data subject is party"[42] or "legitimate interests pursued by the controller or by a third party"[43]are concerned, data processing would be lawful, whether or not consent of the data subject is obtained. This would facilitate business activities that could involve large-scale mining and harvesting of data – to the extent that appropriate contractual

[40]*Supra* note 23, art. 6 §§ 36, cl. 1.
[41]*Id*. Recital 50 §§ 34.
[42]*Id*., art. 6 §§ 34, cl. 1.
[43]*Id.*

obligations or legitimate concerns pursued by the controller are cited. There is, thus, a tendency to prioritise data use benefits by organisations over data privacy of individuals.

D. Personal Data Exchanges

Any counterbalancing of business interests with those of individuals would be incomplete without a true participation of individuals in the data exchange process. A system of Personal Data Exchanges is proposed to this end. This system would not only streamline the data exchange process with clearly defined data privacy provisions, but would also ensure fair value for both producers as well as users of the data. Whereas traditional data protection models emphasise on protection from a purely control and security perspective, the Personal Data Exchange would deal with data as a commodity, aiming to create and regulate the market conditions necessary for a fair exchange.

d) THE RATIONALE

Data exchange processes and laws have so far placed emphasis on the 'flow', 'storage' and 'use' aspects of data. There is a consequential sidelining of the primary process that is the inception point of all subsequent exchanges – that of data generation. By addressing individuals as 'data subjects', the GDPR fails to address their role as primary producers of data. There is a need to shift the conceptualisation of individuals from subjects to generators and, indeed, owners of their data.

The value harnessed by businesses through big data is a direct outcome of the production of this data by individuals. While traditional business models argue that the existing exchange process

ensures fairness by providing for online services (such as Facebook, for example), in return for the collection and analyses of users' data, it is necessary to consider the actual monetary value in profits harnessed by businesses against the sheer extent and invasiveness of data collection activities.

In a market providing generous returns for effective use of big data analytics by businesses, the individual is the starting point and indeed, an indispensable part of the exchange.

e) THE CONCEPT

It is proposed that true individual participation can only materialise through an independent tech-powered platform – a Personal Data Exchange – that allows individuals to store and control the exchange of their data, thereby enabling them to manage their privacy and optionally monetise parts of their online identity. These would represent the fast-growing economies built on personal data – where businesses share the benefits obtained through user data with its primary generators – the individuals themselves.

f) SOME APPROACHES

i. Creating a Primary Market

Wakenshaw, et al. have argued that a "primary exchange economy" could be created upon internalising these externalities. Such a primary exchange does not yet exist because users do not really exchange personal data; rather giving it away in a dual-step process. Firstly, data is generated through their online actions – which could be, for example, by filling up a form online; and secondly, the automatic transferring away of the data – since the technology used for its collection is created and designed to transfer this data right onto the firm's server. The custodial rights for personal data are therefore held by those collecting information about individuals and not by the

individuals themselves.[44] This data then creates a secondary market between firms, as it is sold for aggregators to gain more insights.

However, it is imperative to appreciate that personal data – generated *by* the individual, *through* technology created by the firm – is co-produced. This co-produced entity could be jointly shared between firm and consumer, if an information-processing platform *owned by* the consumers could store and use their data for their own benefit.

Wakenshaw, et al. propose that an easy, enabling access to such data by both firms and consumers would facilitate a more explicit exchange. This would allow for a wider economy of personal data services – one that would preserve privacy as well as provide value to both, firms and users.

ii.Paying Individuals according to their Privacy Attitudes

In another approach, Aperjis and Huberman have held[45] that there is, in principle, no reason why third parties should not pay individuals for the use of their data. They have then proposed the introduction of a realistic market that would allow these payments to be made while taking into account the privacy attitude of the participants.

It is increasingly accepted that markets 'become' through human effort. It is suggested that "the process of market creation is largely a process of institutionalising certain shared understanding and practices of exchange".[46]

The study focuses on the process of 'legitimation' – lending legitimacy to a new market – through both, cognitive legitimation

[44]*See* Shaprio & Varian, *supra* note 30.
[45]Aperjis& Huberman, *supra* note 1.
[46]Wakenshaw et al., *supra* note 3.

(spread of knowledge of a new venture), and socio-political legitimation (acceptance of a venture by public, government etc., as appropriate given existing norms and laws). The legitimation process would result in the legitimacy of these new products, ideas, practices and institutions.

iii.Personal Information Management Systems (PIMS)

The European Data Protection Supervisor (EDPS)[47] has commented that the prevailing circumstances for processing personal data tend to be unfair to the people whose data is processed. It becomes difficult under the prevailing legal conditions and available technical tools for individuals to exercise their rights, allowing controllers to limit the extent of their liability.

Even where formally having been given some form of a 'notice' and opportunity to 'consent' to general terms and conditions, individuals often find themselves inside a system designed to maximise the monetisation of personal data, which leaves no real choice or control to individuals.[48]

The EDPS, in his Opinion 9/2016, has pushed for Personal Information Management Systems (PIMS). This Opinion explores the concept of technologies and ecosystems aiming at empowering individuals to control the sharing of their personal data. The "vision" of the EDPS as discussed in their Opinion 9/2016 is to create a new reality where individuals manage and control their online identity. It aims to transform the current provider centric system into a human centric system where individuals are protected against unlawful

[47]The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.
[48]*Supra.*

processing of their data and against intrusive tracking and profiling techniques that aim at circumventing key data protection principles.

It has been argued that providing access rights to customers would be poised to become an inherent service feature delivered to users, instead of being an administrative burden to be complied with.[49] Organisations based on exploiting 'big data' should 'be prepared to share the wealth created by the processing of personal data with those individuals whose data they process'.[50]

This approach, similar to the one propounded by Wakenshaw, et al. puts individuals as holders of their own data. It visualises a 'paradigm shift in personal data management and processing, with social and economic consequences.'

This is contrasted with the existing model of online services where many small providers are owners of a large amount of personal information – thus dominating the market by monetising individuals' personal information as a trade-off for services. The EDPS has correctly recognized the power imbalance that prevails in this circumstance. There is no real concept of choice as the customer has to deal with a 'take it or leave it' set-up. In the presence of a huge 'information asymmetry', there is negligible transparency for users as to what really happens to their personal data.

[49]European Data Protection Supervisor Opinion 7/2015 – Meeting the Challenges of Big Data
[50]*Id.*

The core idea behind the PIMS concept is to transform the current provider centric system into a system centred on individuals able to manage and control their online identity.[51]

At the core of PIMS lies, what the EDPS refers to as 'consent management' – a function that would bring about an automated matching of consumer preferences with requests by providers for personal data. Sufficient detail would be adhered to in expressing privacy preferences after considering a complex collection of possible options. Periodic updating of privacy preferences of customers in this system would ensure that only the most accurate representation of their privacy and risk attitudes is adhered to.

Aperjis and Huberman in their approach have also advocated for differential pricing based on varying risk attitudes – which would enable a fair-pricing mechanism for personal information, for both users and firms. The two approaches are connected in their classification based on privacy preferences and risk attitudes of users. In the process of developing an exchange system – privacy attitudes, therefore, emerge as an important point of consideration.

As a platform incorporated into a model law for the EU, PIMS will ensure compliance with the GDPR for any transfer of personal data beyond the borders of the Union. Creation of similar systems in other jurisdictions will empower users to decide the geographical extent to which they want their data to be shared. It is here that the system will act as a gatekeeper to ensure that the privacy preferences of the user are met. When seen in context of the differential pricing approach, users who allow for a greater geographical net beyond their immediate boundaries for their personal information may be compensated more than others.

[51]*See* Recital 7 GDPR: 'Natural persons should have control of their own personal data'. See also, for example, Doc Searls, The Intention Economy: When Customers Take Charge (Boston: Harvard Business Review Press, 2012).

IV. THE WAY FORWARD

The lacunae in the 'notice', 'consent' and 'pseudonymisation' provisions, as well as others that may emerge upon implementation should be filled with appropriate revisions, which would then serve as a springboard for a consumer-centric approach to the data exchange process. While the implementation of the GDPR is yet to be seen, policymakers must embark on the next steps to chalk out a regulatory framework for Personal Data Exchanges. This will involve – both, market creation and legitimisation – as well as setting fair and appropriate pricing mechanisms.

With promising research emerging in the area of Personal Data Exchanges, it is important that regulatory bodies take into account the next logical step in data protection – ensuring fairness and equity. Personal information should not lose its essence as a user-owned commodity, and its exchange for services should not be seen as an end in itself. In fact, the only means of ensuring that the Fourth Industrial Revolution corrects the imbalances of the earlier ones is through facilitation mechanisms that achieve the three goals of data protection – security, sharing, and monetising – together.

The emerging landscape of PIMS, aiming at putting individuals and consumers back in control of their personal data, deserves consideration, support and further research with a view to contributing to a sustainable and ethical use of big data and to the effective implementation of the principles of the recently adopted GDPR.[52]

[52] *Id.*

AGROCHEMICALS AND DATA EXCLUSIVITY

*Priyadarshini Singh**

Abstract

This paper seeks to study data exclusivity with particular reference to Indian agro-chemical products. The authors try to define data exclusivity and offeran interpretation of Article 39 of TRIPS agreement in light of data exclusivity to agro-chemical products. The paper examines the Indian position and perspective of data exclusivity by discussing the Satwant Reddy Committee Report. The author also highlights the debate pertaining to IP protection and agrochemicals in Indian scenario. The article also discusses the recent developments in India and around the globe in data exclusivity and agricultural chemicals.

I. INTRODUCTION

There are only three things that can kill a farmer: lightning, rolling over in a tractor, and old age.[1]

*Priyadarshini Singh is a postgraduate student at Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology, Kharagpur. The author may be reached at priyadarshinisingh92@gmail.com.

[1]Bill Bryson, BRAINY QUOTE, http://www.brainyquote.com/quotes/quotes/b/billbryson390788.html? src=t_farmer; although this statement is no longer valid as the underlying theme may also be one of the causes of farmers' death.

Agriculture is a lifeline for the majority of households in India. Over 58 percent of rural households are dependent on agriculture as a sole source of income. Agriculture, along with fisheries and forestry, contributes to the Gross Domestic Product (GDP).[2] The agricultural sector remains the most significant livelihood provider in India, especially in rural areas. It engages a lot of manual power and the efforts from the various sectors. Government policies have played very central role when it comes to agriculture and these have been framed around the agricultural setup.[3] Apart from the factors like weather, seeds, equipment, fertilizers; pesticides are an essential part of agriculture. The agriculture sector is driven by many other interdisciplinary factors, one of them being intellectual property protection. Agriculture and IP has been a naïve relation but wide enough to cajole Plant Verities, farmers 'Right's, biodiversity etc. The government policies play an important role in upliftment of Indian agriculture sector but its fails to acknowledge and address the issues like IP protection relating to agrochemicals which have taken vital position in modern agricultural setup. This paper talks about this very relation and the action taken in its furtherance.

II. DATA EXCLUSIVITY AND AGRICULTURE

The development of a new agrochemical, such as a pesticide or fertilizers usually requires elaborate testing, in the laboratory or the field, on plants, or the environment, depending on the nature of the chemical and its functionality. Data exclusivity also termed as

[2]Indian Agriculture Industry: an overview as per a report jointly presented by Tata Strategic Management Group (TSMG) and FICCI, http://www.ibef.org/industry/agriculture-india.aspx.

[3]*See* https://data.worldbank.org/indicator/SL.AGR.EMPL.ZS; *see also* Total workforce vs. Agricultural Workforce (2011-12) at http://ficci.in/spdocument/20550/FICCI-agri-Report%2009-03-2015.pdf.

regulatory data protection, has a major role when we talk about the development of new agro-chemicals. According to the European Commission:

> *"Data exclusivity" refers to the period during which the data of the original marketing authorisation holder relating to (pre-) clinical testing is protected. Accordingly, in relation to marketing authorisation applications submitted after 30 October 2005 for the applications filed in the framework of national procedures or 20 November 2005 for applications filed in the framework of the centralised procedure, 'data exclusivity' refers to the eight-year protection period during which generic applicant may not refer to the information of the original marketing authorisation holder and 'marketing exclusivity' refers to the ten-year period after which generic products can be placed on the market. However, in relation to marketing authorisation applications submitted before the above mentioned dates, the wording 'data exclusivity' refers to the six or ten-year protection period granted to the original marketing authorisation (MA) holder before generic applicants can file their applications for marketing authorisation".*[4]

These tests serve as the basis on which the effectiveness of the chemicals is ascertained. These trials are conducted in the later stage as per the rules and regulations set by regulating authorities. Meeting all these procedural and developmental requirements is necessary to acquire permission to release the products in the market, which involves enormous cost. It is estimated that the average development cost of agro-chemicals is more than US$180 million.[5]

[4]European Commission, *Pharmaceutical Sector Inquiry, Preliminary Report (DG Competition Staff Working Paper)*, 17 (28 November 2008).
[5]CropLife International, 2004. *Position Paper: On the Protection of Safety and Efficacy Data for Existing and New CropProtection Chemicals*. CROP LIFE

Due to massive investment in clinical test data, agrochemical industries discourage the use of clinical experimental data by third parties. They argue that if this data is made available to other competitors or players and permission is granted to them based on the said test data then recovering the R&D costs involved in the process of evolving a new agrochemical drops exponentially. Relying on this data, if other companies enter the market with an equivalent product, then the profit or incentives of the original company would be jeopardized. The rule to prevent the use of this data by a third party has the effect of providing exclusivity to the original producer which is mostly because the cost of replicating the investment in trials to meet the regulatory requirements would be deterrent and discourage a potential competitor from entering the market.

Data exclusivity usually emphasizes on, preventing regulators from using the clinical trial data which had been the basis of approval for the original product, and supporting the chemically (or otherwise) equivalent generic product. So if a generic company needs approval during this exclusivity period (generally 5-10 years), it will have to carry out all the clinical trial again which will which will cost the same amount of time and money. If the period of data exclusivity overlaps with the patent duration, there is no effect where the patent would prevent generics from releasing the product. Hence, the relation of data exclusivity with agricultutre is very crutial as it governs the very essential tool used in modern agriculture.

III. DEBATED INTELLECTUAL PROPERTY PROTECTION FOR AGROCHEMICALS

India Patent Act, 1970 is TRIPS compliant, and data exclusivity seems to be a TRIPS-plus measure. Article 39.3 is the relevant TRIPS provision to be looking at here. It states:

> *"Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. Also, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."*

The text mentioned above includes the protection of test data against 'unfair commercial use,' but TRIPS agreement does not define the practices that would constitute unfair commercial use and so does the TRIPS member states. Moreover, the disclosure of data is permitted only in two circumstances:

1) Where it is necessary to protect the public,

2) Where data is protected from unfair commercial use.

Various developing countries, including India, interprets Article 39.3 to provide certain minimum standards concerning 'non-disclosure' obligations, usually termed 'data protection' as opposed to 'data exclusivity.' This 'non-disclosure' commitment allows for a permitted reliable standard, leaving it open to national regulators to rely upon the test data submitted to them by originators for marketing approval

for the new applicants.[6] Whereas developing countries aggressively argue that this provision mentioned above is a data exclusivity provision, but when we look into the negotiating history of TRIPS, two clauses were proposed which dealt with data exclusivity but subsequently removed before the final draft was made.[7] Charles Clift[8] views Article 39.3 as being about *data protection*. He writes,

> *"Article 39(3) does not create new property rights, nor a right to prevent reliance on the test data submitted by an originator for the marketing approval of an equivalent product by a third party, except where unfair commercial practices are involved. The article is an articulation of widely accepted legal precepts regarding trade secrets and unfair competition, not an invitation to create a new intellectual property right for test data."*[9]

While some commentators have argued the third position - that Article 39.3 points to a middle-path requiring a compensatory liability

[6]UNCTAD-ICTSD, RESOURCE BOOK ON TRIPS AND DEVELOPMENT (Cambridge University Press, 2004) [hereinafter Unctad-Ictsd Resource Book]; CARLOS MARIA CORREA, PROTECTION OF DATA SUBMITTED FOR THE REGISTRATION OF PHARMACEUTICALS: IMPLEMENTING THE STANDARDS OF THE TRIPS AGREEMENT, SOUTH CENTRE (2002) [hereinafter Correa- South Centre].

[7]Jerome H. Reichman, *Undisclosed Clinical Trial Data Under The Trips Agreement And Its Progeny: A Broader Perspective*, Duke University Sschool of Law.

[8]Charles Clift is chair of the Medicines Patent Pool, a Swiss charitable foundation seeking to increase access to medicine for people living with HIV in developing countries. For a large part of his career he worked as an economist in the UK Department for International Development with experience of working in Kenya, India and the Caribbean. From 2004 to 2006 he was a staff member of the World Health Organisation (WHO). In addition to his work for Chatham House, he has been a consultant to the WHO, UNITAID, the World Intellectual Property Organisation and the Access to Medicine Foundation.

[9] Charles Clift, *Data Protection and Data Exclusivity In Pharmaceuticals and Agrochemical*, Chapter No. 4.9

regime. Prof Correa[10] and other experts have interpreted Article 39(3) to be one of where the regulator simply has to ensure 'non-disclosure' of test data to other private players but can rely on originator's data to give regulatory approval. The fundamental concern posed by data exclusivity is access and affordability. And agrochemicals being at its centre makes it more sensitive.

IV. INDIAN POSITION ON DATA EXCLUSIVITY OF AGROCHEMICALS

Due to mounting pressure of Free Trade Agreements, the Department of Chemicals and Petrochemicals constituted an inter-ministerial committee (including external experts) known as Satwant Committee in February 2004 to assist them.[11]

The Satwant Committee interpreted that Article 39.3 provides two types of protection[12], namely- trade secret protection and data exclusivity. Trade secret protection means protection of data which is submitted to the regulatory authority for registration of unauthorized use or disclosure but can rely upon this information to grant marketing approval to a subsequent application for similar products without disclosing the confidential information. Whereas data exclusivity protection implies non-disclosure and non-reliance on the data from original applicant's test for granting of approval to

[10]Carlos María Correa, *supra* note 6, (From 1984-89, he was Under-secretary of State for Informatics and Development in the Argentine national government. During this period he was the coordinator of the Inter-ministerial Group on Intellectual Property. He was also from 1988 to 1991 government delegate in international negotiations on intellectual property (including the Washington Treaty on integrated circuits and the TRIPS Agreement).

[11]Office Memorandum No.11025/7/2003-PI-II, Government of India, Ministry of Chemicals and Fertilizers,
Department of Chemicals and Petrochemicals, New Delhi, (19th Feb. 2004).

[12]*Id*., ¶ 1.6, pp. 3-4.

subsequent applicants. Further, the committee says that many developed countries accept data exclusivity measures to comply with Article 39.3, but the actual reason behind this acceptance is that these countries majorly incorporate it as policy measure which is an essential requirement of Foreign Trade Agreements.

The Committee suggests that there are some agrochemicals, mainly biotech agrochemicals, where it is hard to make generics, so if protection is given to these drugs, then it will difficult for generics to enter the market. But the committee erred in considering that generic manufacturing difficulties would not affect the innovator company. The committee suggests that inclusion of data exclusivity would be a helpful measure to check the menace of spurious chemicals and pesticides, as only companies with excellent quality of products and resources will be allowed to enter the market during the period of protection.

V. COMMITTEE REPORT ANALYSIS AND POLITICAL BACKDROP

It is argued that the committee did differential treatment to agrochemicals, i.e., a period of three years data exclusivity is not based on any statistics or common understanding. The only reason the committee permitted this is, due to the presence of "me-too" products in the market. The original companies are not able to accumulate the requisite profit which is an equivalent argument favoring data exclusivity for pharmaceuticals products (which finds its mention in the said report). Hence the reason by the committee for agrochemical data exclusivity measure does not justify this differential treatment, and this evaluation is not meaningful.

Committee emphasizes on the environmental impact toxic agrochemical substances might have/ will have. As the committee talks about the pharma and agrochemical industry, it warrants data exclusivity but fails to take into consideration the delicate relationship of reliance in which consumers of agrochemicals are placed, and it goes on justifying data exclusivity policy measure by mitigating risk in agrochemical industry. Also, the committee related the marketing strategy, i.e., door to door marketing with data exclusivity, which is poles apart and such costs have very little to do with data submitted.

The Reddy committee report in 2007 recommended an amendment to Insecticides Act, 1968 for incorporation of a three-year data exclusivity period for agrochemicals, which was mainly done under pressure from big players and not in order comply with TRIPS mandates which was supposed to be as per those mandates. The Pesticides Management Bill, 2008[13]was introduced which had a data exclusivity provision:

> **Section 12:***(6) The data submitted for registration in respect of a pesticide under this section which has not been previously registered shall not be relied upon for grant of registration of the same pesticide in respect of any other person for three years.*
> *(7) Subject to sub-section (6), where a pesticide has been granted a patent, the termof non-reliance on data shall be limited to the duration of the patent.*
> *Explanation: The words "not been previously registered" in respect of a pesticide shall include its name or label expansion through "new uses": Provided that the provisions of non-reliance on data submitted for registration of a pesticide by the first*

[13]Bill No. XLVIII of 2008, http://www.prsindia.org/uploads/media/1224668021/1224668021_The_Pesticides_Management_Bill__2008.pdf.

> *registrant shall be available for the period with effect from the date of the first marketing approval granted anywhere in the world and this shall not apply to the data relating to bio-efficacy and shelf-life part of pesticides where data is to be generated for use under Indian conditions.*
> *(8) Subject to the provisions of sub-section (6), the Central Government may relax or exempt the provision of non-reliance of data submitted for registration of a pesticide by the first registrant in the following circumstances, namely:*
> *(i) (a)national emergency; or*
> *(b)In cases of urgency; or*
> *(c)public interest; or*
> *(ii) for use by the Government for academic and research purposes*

The Bill mentioned above was referred to a Standing Committee of the Parliament which was headed by Samajwadi Party MP, Mr. Mohan Singh. He submitted his report to parliament on 17th February 2009. Paragraph 14 of Reddy Committee's report was acknowledged with an amendment to increase the data exclusivity period for five years instead of 3 years. The reason given for this term extension was, as to encourage the evolution or introduction of newer pesticide molecules in the country. However, **the BJP opposed the Bill then,**[14] stating:

> "certain clauses had been inserted in it under pressure from the West and were inimical to the country's interests.*" and* "Under the data exclusivity provision, the researcher's data

[14]THE ECONOMIC TIMES (May 06, 2010), http://articles.economictimes.indiatimes.com/2010-05-06/news/28475814_1_data-exclusivity-saffron-party-bharatiya-janata-party.

> will be his monopoly, and no one else in the world would be allowed to have control over it. "Monopoly can also lead to exploitation and a hike in the prices of pesticides. Such a clause will have dangerous consequences for the developing countries such as India," a senior leader argued."

Also, the Parliamentary Standing Committee[15] stated in its 88th report that the impacts of data exclusivity are quite severe and grave and the Standing committee strongly recommended that:

> "the Government should not fall prey to such demands of MNCs. The Government must thwart such attempts, being made at the behest of certain vested interests. It should guard against moves to enter into FTA with the USA, as the developed countries, particularly the USA, are trying to bring in certain TRIPS-Plus measures through Bilateral and Regional Agreements."

Meanwhile, the Bill was pending; the Government passed two notifications which talks about implementing data exclusivity under the Insecticides Act are as follows:
(i)No.17-2/2006-PP.I dated 30th October 2007
(ii)F.No.17-2/2006-PP.I dated 18th February 2008

Further, in Syngenta India Ltd vs. Union of India[16], Justice Bhat[17] questioned the legality of these notifications and opined that:

> *"*There is no statutory guidance, either in the substantive portion of the enactment or under the Rules, enabling even the rulemaking authority to prescribe a period of limitation for "data exclusivity."

[15]Standing Committee On Agriculture, http://164.100.47.134/lsscommittee/Agriculture/88th%20 report.pdf (2008-09).
[16]Syngenta India Ltd v. Union of India, W.P. (C) 8123/2008.
[17]http://lobis.nic.in/dhc/SRB/judgement/02-07-2009/SRB01072009CW%2081232008.pdf.

The Bill was back for consideration by the same party which once opposed it. This act of taking up the bill to the table for discussion by BJP might be assessed as to be done with an intention to give assurance to US/EU of its "good-intention" without acknowledging as what cost the country have to pay for doing the same. If this attitude by the Government persists then, patent linkage[18] In India might become a reality soon without proper consideration of its harmful effect on the country.

The whole story of Agrochemicals and data exclusivity debate related to it seems like a political story rather than an honest effort by the government to consider the issue and take up the matter seriously. The political backdrop tells about the good will establishment by the parties and not the data exclusivity issues which were claimed to be addressed.

VI. CONCLUSION

As stated initially in this article, the introduction of a data exclusivity provision with regard to agrochemicals was never established on any data-based study so there is a need for robust empirical, evidence-based policy and rethinking the whole argument of data exclusivity and its term. The author suggests that data exclusivity provisions will bring more agrochemicals in the market or cause an increase in the FDI, must be shown. As Prof. Shamnad Basheer[19] has discussed,[20] it

[18]Patent linkage refers to the system or process by which a country links drug marketing approval to the status of the patent(s) corresponding to the originator's product.

[19]Prof. Basheer is the founder of Increasing Diversity by Increasing Access to Legal Education - a trust which works on making legal education accessible to underprivileged students. Basheer was a Ministry of Human Resource Development Chaired Professor of Intellectual Property Law at the West Bengal

is very likely that such a provision would help foreign countries receive more money and not give the claimed benefit to the host country, so India needs to reconsider the agrochemical market and also the data exclusivity debate related to it.

The author is of the opinion that the regulatory issues need to be fixed and needs revision. Also, a pseudo proxy mechanism based on lobbying can be considered if relying on empirical evidence is not possible. It extends the monopoly periods of products and makes these products inaccessible.It will serve as a progressive ladder for some multinational to start demanding data exclusivity for agrochemicals– which will, in turn, make pesticides harder to access. These actions of India will be giving an impression that it is stepping down from its strong stance of a balanced IP regime and giving into the demands of big multinational companies, which in turn effects its economy, which is agriculture dependent. Therefore, the agrochemical players and the government need to look again into the regulatory provisions and requirements.

National University of Juridical Sciences, Kolkata, and the Frank H. Marks Visiting Associate Professor of Intellectual Property Law at the George Washington University Law School and a research associate at the Oxford Intellectual Property Research Center (OIPRC). He founded several initiatives such as SpicyIP, IDIA, P-PIL and Lex Biosis. Basheer had intervened in landmark Novartis case and filed some other public interest litigation and took the initiative to bring about changes in IPR regime in India.

[20]SpicyIP, *Data Exclusivity Debate: Whither Context*?, http://spicyip.com/2011/02/data-exclusivity-debate-whither-context.html.

ADJUDICATING CYBER ESPIONAGE CASES THROUGH THE WORLD TRADE ORGANIZATION'S DISPUTE SETTLEMENT SYSTEM

*Roshni Ranganathan**

Abstract

In 2013, United States received a report that revealed cyberattacks by the Chinese military on U.S. companies to steal their trade secrets in order to provide leverage to domestic Chinese companies. The legal recourse available to states in such circumstances is unclear and thus, requires some discussion. Stealing of trade secrets to provide some competitive advantage to one's own companies can be understood to mean commercial or economic cyber espionage. No international treaty governs economic espionage specifically but a basic protection to trade secrets[1] and other intellectual property is provided through the World Trade Organization's (WTO) Agreement on Trade

*Roshni Ranganathan is a fifth year student at Gujarat National Law University, Gandhinagar. The author may be reached at roshniranganathan@gmail.com.

[1]TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), art. 39.2 [hereinafter 'TRIPS Agreement'].

Related Intellectual Property Rights (TRIPS)[2]*, which can be extended to protect the confidential data of the companies which gives them the trade advantage.*

Keeping this in mind, the author seeks to analyse the possibility of litigating commercial cyber espionage complaints through the WTO Dispute Settlement Body (DSB) as a ***TRIPS violation*** *and as* ***a non-violation complain****. These concepts are explained through the above* ***case study*** *of United States and China with respect to alleged acts of economic cyber espionage by China on U.S. By applying the relevant provisions of TRIPS and GATT 1994, the author will establish that among the few alternatives that are available to the United States for addressing and adjudicating commercial cyber espionage, WTO may not be the best forum for disputing data protection given the present system in existence. In order to serve as an adjudicatory forum, WTO must reconsider its existing mechanism to either modify TRIPS or formulate a new agreement that specifically addresses cyber espionage issues in trade.*

[2]TRIPS Agreement, art. 42.

I. INTRODUCTION

The modern global economy thrives on data. With an increase in the amount of data being collected and transferred on a daily basis, instances of cyber espionage are also on the rise.[3] One form of espionage is economic espionage which involves attempts by a state to covertly acquire trade secrets held by foreign private enterprises.[4] Protection against such espionage has been long considered by countries as important to national security and economic development.[5] With the advent of Internet, cyber economic espionage has become a growing concern among many countries.[6]

While countries like U.S. have their own national laws[7] governing cyber espionage, there is no international norm or treaty that addresses this issue at a global level.[8] In the absence of such a norm or treaty, some countries have entered into agreements with other countries to prevent theft of data from within their borders, such as the agreement entered into between U.K. and China to "not engage in commercially motivated cyber espionage."[9] However, such diplomatic agreements are not legally binding as they do not have the

[3]David J. Kappos and Pamela Passman, *Cyber Espionage is Reaching Crisis Level*, FORTUNE (December 12, 2015), http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/, (last visited Feb. 18, 2018).
[4]David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 INSIGHTS AMERICAN SOCIETY OF INT'L L 10 (2013), https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.
[5]*Id.*
[6]David J. Kappos and Pamela Passman, *Cyber Espionage is Reaching Crisis Level*, FORTUNE (December 12, 2015) http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/, (last visited Feb. 18, 2018).
[7]Economic Espionage Act, 18 U.S. Code § 1831 (1996).
[8]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE (December 4, 2015) https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).
[9]*Id.*

sanction of a treaty. This article, therefore, looks into the viability of contesting cyber economic espionage at the WTO's Dispute Settlement Body as an alternative given that the states are bound by the decisions of the WTO Panel or Appellate Body[10] and the obligation to protect undisclosed information under TRIPS Agreement.[11]

Commercial cyber espionage, which is the focus of this article, specifically relates to a state's cyber activities to obtain trade secrets from foreign companies with the intent of providing competitive leverages to domestic companies.[12] For example, if companies belonging to State A carry on business in State B and have subsequently become targets of data theft by actors in State B, it compromises their competitiveness in State B and worldwide. Such acts amount to commercial cyber espionage.[13]

Although no international treaty governs economic espionage specifically, a basic protection to trade secrets[14] and other intellectual property is provided through World Trade Organization's (WTO) Agreement on Trade Related Intellectual Property Rights (TRIPS).[15] This Agreement can be extended to accord protection to the

[10]World Trade Organisation, *Dispute Settlement without recourse to Panels and the Appellate Body*, https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c8s1p1_e.htm, (last visited Feb. 17, 2018).
[11]TRIPS Agreement, art 39.
[12]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE (November 30, 2017), https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).
[13]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 1 (2015).
[14]TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), art. 39.2 [hereinafter 'TRIPS Agreement'].
[15]TRIPS Agreement, art. 42.

confidential data that provides the concerned company with a trade advantage.

As things stand at present, there is a lack of clarity with respect to the actions that a victim state may take in case of commercial cyber espionage. The United States (U.S), for example, resorted to imposing unilateral trade sanctions on North Korea after a cyber attack by the latter state on Sony Pictures, an entertainment company based in U.S. A hacker group going by the name "Guardians of Peace" identified themselves as the perpetrators behind the attack where a great amount of confidential information of Sony Pictures, including employees' Social Security Number, e-mail address, etc. was leaked online.[16] The attack was attributed to North Korea and the purpose was to prevent them (Sony) from releasing the movie "Interview", which allegedly ridiculed the leader of North Korea, Kim Jong-Un.[17] In retaliation, United States imposed limited economic sanctions on North Korea. It was the first time a country had imposed economic and trade sanctions to counter destructive use of cyber space by another country.[18]

Resort to such unilateral measures by the U.S. highlights the lack of any international legal mechanism or other recourses available to states to deal with cyber activities by other state actors. This leads us to some important questions: How can a state protect its confidential data from being stolen by other state actors? And in case of theft of such data or attempt to steal, what recourse would the complaining state have?

[16]Gabi Siboni and David Siman-Tov, *Cyberspace Extortion: North Korea versus the United States*, 646INSS INSIGHT 1-3 (2014).
[17]*Id.*
[18]David E. Sanger and Michael S. Schmidt, *More Sanctions on North Korea After Sony*, N. Y. TIMES, March 1, 2015, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctionson-10-north-koreans.html, (last visited Sept. 28, 2017).

Given the current increase in cross border data flow among countries, there is a need for an international legal system to adjudicate cyber-espionage claims. With the above key questions in mind, this article will examine the viability of adjudicating disputes concerning cyber espionage (in particular, commercial cyber espionage) through WTO's dispute settlement system. For this purpose, the article is divided into four parts, namely:

Part I – Commercial Cyber Espionage by China on U.S. – A Case Study
Part II – TRIPS Violation Claims
Part III – Non-Violation Complaint under GATT
Part IV – Conclusion

Part I introduces the reader to the commercial cyber espionage launched by the Chinese Military on U.S. in 2013. Using this incident as the main case study, the article examines the options that would be available to U.S. (or another state in a similar position) if it were to pursue the matter through WTO's Dispute Settlement Body. These options, in the form of TRIPS violation claims and non-violation claims, have been analysed in detail in Part II & III. Part II discusses the various provisions under TRIPS that are violated by a state when it engages in espionage and analyses if the same were to apply to a case of commercial cyber espionage. Part III, on the other hand, examines whether an act of commercial cyber espionage could give rise to a non-violation complaint under GATT 1994. The article answers both the questions raised in these two parts in the negative. Through this, the author aims to prove that the present mechanism under which the WTO functions is insufficient to provide an effective remedy to a complaining state in the event of commercial cyber espionage. On that note, the article concludes in Part IV with thoughts on whether WTO should amend its existing covered agreements to include commercial cyber espionage as a violation or draft a new

agreement for activities in the cyber space altogether which would include commercial and trade related aspects.

II. COMMERCIAL CYBER ESPIONAGE BY CHINA ON U.S – A CASE STUDY

A. Background

Despite hundreds of billions of dollars being spent on cyber-security, the possibilities of cyber-attacks only seem to grow with time.[19] In 2013 at the Asia Society, U.S. National Security Advisor, Tom Donilon, highlighted the growing global concern with respect to cyber security. He stated:

> *"Cyber-security is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about the sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale…As the President said in the State of the Union, we will take action to protect our economy against cyber-threats."*[20]

His statement reflected the concern of the entire U.S. government regarding the alleged cyber espionage by the Chinese military, which was revealed through a report by a private company in February

[19]Craig Timberg, *A Flaw in the Design*. WASHINGTON POST https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (May 31, 2015).
[20]Tom Donilon, *The Asia-Pacific in 2013*, (Remarks given to the Asia Society, White House Press Office, Washington, D.C., March 11, 2013).

2013.[21] The report stated that the Chinese military had employed cyber technology to steal trade secrets from foreign companies. It was speculated that this was to provide a competitive advantage to domestic Chinese companies as against those foreign companies. Therefore, the competitive advantage of U.S. companies in China *and worldwide* was compromised.[22]

B. Recourse Available to U.S

The existing legal instruments and policies on protection of intellectual property and trade secrets pre-date the advancement of the internet. The Uruguay Round Agreements,[23] which includes TRIPS, was concluded in 1995, when internet had just gained traction. Therefore, to successfully bring an international claim of cyber-espionage in trade against another state calls for creative application of the existing regime, which Prof. Malawer argues is available.[24]

The possible recourse that may be available to the United States is by approaching WTO under TRIPS Agreement or through Article 26 of DSU or by imposing unilateral sanctions on the opposite party (China) as it did in the case of North Korea.

[21]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).
[22]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 1(2015).
[23]*Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations*, Apr. 15, 1994, 1867 U.N.T.S. 14, 33 I.L.M. 1143 (1994), https://www.wto.org/english/docs_e/legal_e/03-fa_e.htm., (last visited Sept. 30, 2017).
[24]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 2 (2015).

III. TRIPS VIOLATION CLAIMS

The TRIPS Agreement [hereinafter 'TRIPS'], does not explicitly provide for protection against economic cyber espionage for commercial or competitive advantages. However, it interesting to note whether and how the existing provisions of TRIPS may be creatively applied, especially in the U.S.-China case described above.

A. Preamble

The basic objective of TRIPS, reflected through its preamble, is "to reduce distortions and impediments to trade... taking into **account the need to promote effective and adequate protection of intellectual property rights**, and to ensure that measures and procedures to enforce intellectual property rights do not themselves become barriers to legitimate trade"[25] [*emphasis supplied*].

This text recognizes that lack of adequate protection to IP rights restricts trade[26] and leads to free rider problems.[27] Given that there are no specific laws governing the aspects of trade secret theft in the form of cyber espionage, the objective of TRIPS could come to its rescue. One can argue that if the underlying objective of TRIPS is to ensure adequate protection to IP, then the corollary is that it needs to be extended and applied to protect those IP aspects that were not envisaged at the time of negotiating the Agreement. However, such an argument fails to recognize the importance of the substantive provisions. While the objective of the TRIPS is correctly stated, it

[25]TRIPS Agreement, preamble.
[26]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION 744 (2d ed. 2009).
[27]T. Cottier, *The Agreement on Trade Related Aspects of Intellectual Property Rights*, THE WORLD TRADE ORGANISATION: LEGAL, ECONOMIC AND POLITICAL ANALYSIS 1054 (Springer, 2005).

cannot be applied in isolation to include protection against commercial cyber espionage.

Therefore, it becomes important to understand the scope of application of the TRIPS Agreement as it currently exists.

B. Scope of Application

Article 1.2 of TRIPS provides that: "For the purposes of this Agreement, the term 'intellectual property' refers to all categories of IP that are the subject of Sections 1 through 7 of Part II." These subjects are:

a. Copyright and related rights;
b. Trademarks
c. GI
d. Industrial Design;
e. Patents
f. Layout-designs of ICs;
g. Protection of undisclosed information.

Plain reading of Article 1.2 implies that not all forms of IP rights are covered by TRIPS. However, these categories are not clear cut. In *U.S. – Section 211 Appropriations Act*, the Panel was faced with interpreting Article 2.1 of TRIPS in relation to 'trade names', which though not explicitly covered by the above-listed subjects, was covered under Article 1(2) of the Paris Convention. The Panel opined that the Paris Convention would not apply as the list of subjects from Sections 1-7 was exhaustive because Article 1.2 of TRIPS refers to 'all categories'.[28] The Appellate Body, however, differed on this. It held that the scope of application of TRIPS is "not limited to the categories indicated in each *title* but with other *subjects* as well"[29]

[28]Panel Report, *US – Section 211 Appropriations Act*, ¶ 8.26.
[29]Appellate Body Report, *US – Section 211 Appropriations Act*, ¶ 335.

implying that TRIPS also covers those IP rights in other conventions that incorporate the 'subject' of these Sections.[30]

In the present context, cyber espionage of trade secrets clearly falls within the last category, i.e. 'protection of undisclosed information'. However, should one argue that cyber espionage is not explicitly covered, the above interpretation by the Appellate Board widens the scope of the TRIPS Agreement to include several other aspects related to these subjects.

If trade secret protection against commercial cyber espionage is not covered by TRIPS, no remedy will lie in the WTO Dispute Settlement System. United States can successfully bring a claim against China only when it can prove that an obligation, like national treatment, for example, exists in relation to the IP right claimed.

C. National Treatment Principle – Article 3

National treatment is one of the major principles in international trade law[31] and intellectual property.[32] It reads as follows:

> *"Article 3*
>
> *National Treatment*
>
> *1. Each Member shall accord to the nationals of other Members treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property, subject to the exceptions already provided in,*

[30]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION, 751 (2d ed. 2009).
[31]M. MATSUSHITA & T. F. SCHOENBAUM & P. C. MAVROIDIS, THE WORLD TRADE ORGANISATION: LAW, PRACTICE, AND POLICY, 233 (2nd ed. 2006).
[32]F. H. Reichman, *Universal Minimum Standards of Intellectual Property Protection under the TRIPS Component of WTO Agreement*, 29 INT'L L.J. 2, 345, 347 (1995).

> *respectively, the Paris Convention (1967), the Berne Convention (1971), the Rome Convention or the Treaty on Intellectual Property in Respect of Integrated Circuits. In respect of performers, producers of phonograms and broadcasting organizations, this obligation only applies in respect of the rights provided under this Agreement. Any Member availing itself of the possibilities provided in Article 6 of the Berne Convention (1971) or paragraph 1(b) of Article 16 of the Rome Convention shall make a notification as foreseen in those provisions to the Council for TRIPS.*
>
> *2. Members may avail themselves of the exceptions permitted under paragraph 1 in relation to judicial and administrative procedures, including the designation of an address for service or the appointment of an agent within the jurisdiction of a Member, only where such exceptions are necessary to secure compliance with laws and regulations which are not inconsistent with the provisions of this Agreement and where such practices are not applied in a manner which would constitute a disguised restriction on trade."*

The main objective of this provision[33] is to eliminate discrimination between a foreign person and a national with respect to protection of intellectual property.[34] The relevant question then is whether this protection extends to prevent a member state from (unlawfully) procuring the trade secrets and other IP information from foreign firms *within its territory* and then pass on such information to its nationals/domestic firms? The answer to this is in the affirmative as is

[33]TRIPS Agreement, art. 3 – "Each Member shall accord to the nationals of other members treatment no less favorable than that it accords to its own nationals with regard to the protection of intellectual property."
[34]M. Matsushita & T. F. Schoenbaum & P. C. Mavroidis, *supra* note 32, at 233 (2nd ed. 2006).

clear from a plain reading of the provision. However, this protection is territorial in nature.[35]

Given that the treatment of foreign IP is dependent on the extent of rights and protection granted to a national under the domestic law, this provision does not extend the obligation of the member state to firms outside its territory. In other words, if a member state secures trade secrets of a foreign firm (that is not situated within its territory) in order to provide benefits to its domestic firms from such secrets, the member state to which the foreign firm belongs cannot claim national treatment violation. Some scholars disagree on this point.[36] They claim that if the effects and benefits of the stolen information accrue to the intruding state, then such actions are also reasonably included within the language of Article III.[37] That is to say, if it can be proved that Chinese firms benefitted from the stolen information or the effects of such theft accrued to China, then U.S. can claim violation of national treatment principle under TRIPS. However, there is nothing provided in the WTO Agreement or in the TRIPS Agreement that extends the obligation of a member state to protect the confidential information of companies outside its territory.[38] More generally, even international law does not prohibit economic espionage either through treaty or customary international law.[39]

[35]Loewenheim U, *The Principle of National Treatment in the International Conventions Protecting Intellectual Property*, In: Pyrmont W.P.W., Adelman M.J., Brauneis R., Drexl J., Nack R. (eds) *Patents and Technological Progress in a Globalized World*, MPI STUDIES ON INTELLECTUAL PROPERTY, COMPETITION AND TAX LAW, 6 (Springer, Berlin, Heidelberg 2009).

[36]Stuart S. Malawer, *Chinese Economic Cyber Espionage*, 1 GEORGETOWN J. ON INT'L AFFAIRS 4, 5 (2015) [hereinafter 'Malawer'].

[37]*Id.*

[38]David P. Fidler, *Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage*, *Arms Control Law* (Feb. 11, 2013), https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/, (last visited Feb. 18, 2018).

[39]Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071 (2006).

Therefore, under the existing jurisprudence on WTO and TRIPS, national treatment principle is territorial in nature.

Another issue with claiming national treatment violation as a result of cyber economic espionage is discharging of burden of proof by the complaining party. The problem of attribution is common across all cyber espionage cases, i.e. pinning responsibility on the perpetrator of the attack.[40] If a state is unable to discharge this burden sufficiently, then it is argued that the chances of succeeding in a case of commercial cyber espionage are low. In case of the Chinese cyber espionage on U.S., the latter state relied on reports that were released by a private company while attributing the attack to China.[41] In the absence of any other proof or empirical data, this report alone may not suffice in establishing responsibility on China for the attack.[42] Therefore, a complaint by U.S. alleging violation of national treatment principle by China will not succeed for economic cyber espionage cases.

D. Protection of Undisclosed Information – Article 39

Article 39 of TRIPS imposes an obligation on the member states to protect undisclosed information of natural and legal persons. Paragraph 1 of Article 39 imposes an obligation on the member

[40]C Fred Bergsten, *Bridging the Pacific: toward free trade and investment between China and the United States*; Gary Clyde Hufbauer; Sean Miner, 356 (Washington, District of Columbia: Peterson Institute for International Economics, 2014).
[41]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).
[42]C Fred Bergsten, B*ridging the Pacific : toward free trade and investment between China and the United States*; Gary Clyde Hufbauer; Sean Miner, 356 (Washington, District of Columbia : Peterson Institute for International Economics, 2014); David P. Fidler, *Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage*, Arms Control Law (Feb. 11, 2013), https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/, (last visited Feb. 18, 2018).

states; paragraph 2 provides a right of protection of undisclosed information against disclosure to natural and legal persons (read with Article 39.1) and paragraph 3 deals with data submitted to government or their agencies.

The protection under Article 39.2 is from disclosures done "in a manner contrary to honest commercial practices"[43] the meaning of which is clarified in the footnote to the provision.[44] It includes breach of contract, breach of confidence, inducement to breach, and acquisition by parties who knew such practices were being employed to acquire such information. Commercial cyber espionage will fall within "breach of confidence" as the confidential information in such cases is obtained without the knowledge of the owner and used without his/her express or implied consent.[45]

The meaning of "honest commercial practices" was further espoused by the Appellate Body in *US – Hot Rolled Steel* case where it stated:

> *"The word 'honest' which qualifies the word 'practices', indicates that... the 'practices' must conform to the dictates of the basic principles of good faith and fundamental fairness."*[46]

This obligation will be breached by any state (China, in the present case) that acquires trade secrets in a clandestine manner[47] in order to

[43]TRIPS Agreement, art. 39.2.
[44]TRIPS Agreement, Note to art. 39: "For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition"
[45]Saltman Engineering v. Campbell Engineering, (1948) 65 RPC 203 (CA).
[46]Appellate Body Report, *US – Hot Rolled Steel,* ¶ 193.
[47]Commonwealth v. John Fairfax & Sons Ltd., (1980) 147 CLR 39, 50.

secure some competitive/commercial advantage to its national companies.[48]

The main task of the complaining state would then be to prove that the information so acquired falls within the parameters of "undisclosed information" as laid down in Article 39.2(a) to (c). These parameters stipulate that the information should be:

> a) Should have been kept a secret through reasonable steps taken by the person in control of the information.[49]
> b) Should have a commercial value attributable to its secrecy;[50]
> c) A secret that is not generally known or readily accessible to the persons who normally deal with this kind of information;[51]

The problem in determining 'reasonable steps' taken to protect the information in case of a digitally protected data is that the complaining party may have to reveal the security mechanisms in place to protect the data which could make the data vulnerable to new attacks. However, unlike domestic dispute settlement bodies, the WTO Panel understands the need for additional protection of business information submitted to Panels.[52] In *Canada – Aircraft* and *Brazil – Aircraft*, the confidential information was to be stored in a locked room at the premises of the relevant Geneva missions, with

[48]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).
[49]TRIPS Agreement, art. 39.2(c).
[50]TRIPS Agreement, art. 39.2(b).
[51]TRIPS Agreement, art. 39.2(a).
[52]PETER VAN DEN BOSSCHE, THE LAW AND POLICY OF THE WORLD TRADE ORGANISATION 284 (2d ed. 2009).

restrictions imposed on access.[53] Special procedures were adopted to govern this information which *inter alia* provided for destruction of the confidential information upon completion of the proceedings. Despite this, Canada refused to submit the confidential information, citing reasons of inadequate protection. The Appellate Body, however, stressed that refusal to provide information shall not be the only determining criteria to draw inferences.[54]

In the context of commercial cyber espionage, when the confidential information is stored digitally, adopting such special procedures and ensuring that they remain confidential becomes difficult. In order to overcome this difficulty, the Procedures Governing Business Confidential Information needs to be amended to suit the needs of the digital age.

Secondly, the information so revealed should have a commercial value.[55] Interpretation of "undisclosed information" under Article 39 encompasses 'company secrets' as well.[56] Private information is not covered given the distinction between confidential information and trade secrets.[57] To claim protection under Article 39, it must be proved that the information affects the competitive advantage of the national.[58] In the context of commercial espionage, this implies that cyber attacks like that on *Sony*are outside the scope of litigation through WTO. In case of economic espionage by the Chinese military, it needs to be proved that the information that was disclosed

[53]Panel Report, *Canad – Aircraft*, Annex 1; Panel Report, *Brazil – Aircraft*, Annex 1.
[54]Appellate Body Report, *Canda – Aircraft*, paras. 204-5; Panel Report, *US – Upland Cotton*, ⁋⁋. 7.20-7.42, 7.609-7.633.
[55]TRIPS Agreement, art. 39.2(b).
[56]M. BLAKENEY, TRADE RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS: A CONCISE GIDE TO THE TRIPS AGREEMENT, 103 (1996).
[57]Faccenda Chicken Ltd v. Fowler, [1986] 1 All ER 617.
[58]WTO – TRADE RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS 635 (Peter Tobias Stoll, Jan Busche and Katrin Arend eds., Max Planck Institute for Comparative Public International Law 2008).

was indeed used to provide the domestic companies with a trade advantage over foreign companies, i.e. U.S. Companies. However, in the absence of any WTO jurisprudence in this regard, it is unclear whether threatening the foreign firm with its confidential information, in order to gain some trade/commercial leverage, would amount to 'acts contrary to honest commercial practices.'

The third parameter is that of 'ready accessibility'. The impugned information should be a secret that is not generally known or readily accessible to the persons who normally deal with this kind of information.[59] This aspect of 'ready accessibility' has been subject to various national interpretations. In case of U.S., the information is considered secret if it requires "considerable difficulties" to access it.[60] In Germany, on the other hand, the time and "effort", and the obstacles in place to prevent disclosure are considered to determine accessibility.[61] The kind of interpretation to be applied to any case would depend on the facts and circumstances of each case.

Even if the state is able to prove the above requirements with respect to the information in question, the problem of territoriality, as seen in case of national treatment, re-surfaces.[62] Scholars argue that the use of the words 'possibility of preventing' in Article 39.2[63] implies that it

[59]TRIPS Agreement, art. 39.2(a).
[60]M. MATSUSHITA & T. F. SCHOENBAUM & P. C. MAVROIDIS, THE WORLD TRADE ORGANISATION: LAW, PRACTICE, AND POLICY, 246 (2nd ed. 2006).
[61]*Id.*
[62]*Supra* Part II, 2.3; C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).
[63]TRIPS Agreement, art. 39.2: "2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and

does not provide a right to a legal claim to the nationals but rather obliges the member states to "provide legal instruments to their nationals to enable them to prevent infringements."[64] This means that Article 39.2 does not grant any exclusive right of protection at an international level[65] but only imposes an obligation on the member states to implement mechanisms that meet the minimum standards which can be done by enacting national laws to that effect.[66] Therefore, in order to successfully prove Article 39 violation, the complainant state must prove that the member state complained of has not met its obligation under TRIPS.

The kinds of obligation recognized under the TRIPS for this purpose are obligation to protect against disclosure and against unfair commercial use.[67] In case of commercial cyber espionage, it becomes important to prove that the confidential data was used for commercial advantage.[68] In the Chinese military attack on U.S., the reports were released by a private company[69] with no concrete evidence to establish that the data has been used by China to provide competitive advantage to the Chinese firms.

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

[64]C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).

[65]World Health Organisation, Protection of Data Submitted for the Registration of Pharmaceuticals: Implementing the Standards of the TRIPS Agreement (2002), § 6.

[66]C. CORREA & A. YUSUF, INTELLECTUAL PROPERTY AND INTERNATIONAL TRADE: THE TRIPS AGREEMENT 370 (1998).

[67]*Id.*

[68]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[69]Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. (last visited Sept. 28, 2017).

Therefore, an action may lie at WTO under TRIPS for acts of commercial cyber espionage only if the foreign firm is within the territory of the violating state and if the complaining state can prove that the information qualifies as 'undisclosed' as required by Article 39. It will be very difficult to provide a remedy at WTO in case the company operates outside the territory of the violating state for reasons explained above.[70]

IV. NON-VIOLATION COMPLAINT UNDER GATT

Filing a non-violation complaint is another avenue that a state can explore. According to the non-violation principle, the member state can approach the Dispute Settlement Body without there being any agreement with the other state complained of. The principle of non-violation is laid down in Article 26.1 of Dispute Settlement Understanding and Article 64.1 of TRIPS. However, currently there is a moratorium (temporary ban) on non-violation complaints on intellectual property claims under TRIPS.[71] Initially this period was for five years (that is, 1995-1999). It has been extended since then.[72] Although there have been arguments from countries like U.S. and Switzerland to make non-violation claim applicable under TRIPS, the majority of the member states either wanted to impose a complete ban on non-violation complaints in respect of IP or extend the moratorium. At the 11th Ministerial Conference in Buenos Aires in December 2017 the member states agreed to once again extend the

[70] *Supra* Part II, 2.3, 2.4.
[71] *TRIPS: 'Non-Violation' Complaints (Article 64.2)*, WORLD TRADE ORGANISATION, https://www.wto.org/english/tratop_e/trips_e/nonviolation_background_e.htm, (last visited Oct. 2, 2017).
[72] WTO: 2015 News Item, Intellectual Property: Formal Meeting, WTO website, November 23, 2015.

moratorium until the 12th Ministerial Conference in 2019.[73] Till then, the members are not permitted to initiate any non-violation complaints under TRIPS.[74]

If the State party wishes to approach the Panel under Article 26.1 of DSU instead of Article 64 of TRIPS, then it (the complaining party) needs to satisfy the three part structure set out by the Panel in *Japan – Film* case-

a) the application of a "measure"

b) the identification of a benefit owing to the complainant under some WTO agreement; and

c) a demonstration that the measure has nullified or impaired that benefit.[75]

Going by the interpretation, it is debateable if acts of commercial cyber espionage constitute a 'measure' for the purpose of non-violation claims. Whether or not "benefits" were owed to the complainant varies with facts and circumstances of the case. For example, if State X collects confidential information from foreign companies within its territory to provide certain commercial advantages to the domestic companies, there could be impairment of benefits. However, when the foreign company do not operate with or within the territory,[76] there are generally no benefits promised by State X to such companies. Does that imply that no obligation is owed by State X to such a company? Under GATT 1994, at least, no such

[73]*TRIPS: 'Non-Violation' Complaints (Article 64.2),* WORLD TRADE ORGANISATION,https://www.wto.org/english/tratop_e/trips_e/nonviolation_e.htm, (last visited Feb. 28, 2018).
[74]*Id.*
[75]Panel Report, *Japan – Film.*
[76]"with" includes export-import activities with that state and "within" includes establishing a physical presence in that territory.

obligation can be traced to State X in the absence of any 'benefits' promised to the complainant state.

Further, under Article 26.1(b) of DSU, the Appellate Body does not require the 'measure' to be withdrawn by the state complained of in case it nullifies or impairs the benefits, but can only*recommend* the parties to make a 'mutually satisfactory agreement'.[77] This means that the member state complained of does not have an obligation to withdraw or discontinue the measure involving cyber espionage. The WTO can merely recommend China and U.S. to reach a mutually satisfactory agreement. This will not be a satisfactory remedy for cyber espionage cases as it does not stop the violating state from stealing confidential information. It is probably in this light that U.S. and China entered into an agreement to refrain from carrying on any cyber-related theft of confidential information.[78]

At the time when this incident came to light, many cyber-security experts discussed that U.S. could claim national security exception under Article XXI of GATT, 1994 and subsequently impose unilateral sanctions on China.[79] However, there has been no case till date in the WTO where the parties have claimed this exception.[80] Therefore, it is difficult to ascertain if such a strategy would succeed.

V. CONCLUSION

[77]GATT 1994:General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994), art. 26.1(b) [*hereinafter* 'GATT 1994'].
[78]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).
[79]James Andrew Lewis, Center for Strategic and International Studies, Conflict and Negotiation in Cyberspace 50 (Feb. 2013).
[80]Malawer, *supra* note 36.

The U.S-China cyber economic espionage dispute amplifies the absence of any straightforward or uniform adjudication process for a state to undertake in case of such an occurrence. Through the above analysis, this article proves that an action by the U.S against China at WTO would not have been successful. Considering these difficulties in adjudicating the matter at WTO at present, U.S. probably availed the right alternative by entering into an agreement with China in September 2015 (also known as Xi-Obama Agreement) to not engage in economic cyber espionage activities against each other.[81]

The agreement states:

> *"that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."*[82]

Subsequently, China entered into a similar agreement with United Kingdom as well.[83] Not long after, a G-20 communiqué extended the Xi-Obama agreement to 18 other countries.[84] In the absence of any international law on cyber espionage, many scholars acknowledged

[81] Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?* LAWFARE https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm.

[82]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).

[83]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).

[84]Martin Libicki , *The Coming of Cyber Espionage Norms*, NATO CCD COE PUBLICATION, Tallinn 1, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espi nage%20Norms.pdf, (last visited Feb. 20, 2018).

this trend as an emerging norm in international law.[85] In other words, the practice of entering into agreements with other states to prevent economic cyber espionage was becoming increasingly recognized and accepted in the international community.[86] If such a practice attains the status of an international norm, then no derogation from the same would be permissible.[87] It received sufficient support at the G-20 Summit in November 2015 to be recognized as an international norm according to international law experts.[88] However, in practice, such diplomatic agreements go only so far as to enforce a legal order on cyber espionage. They as are not binding on the parties as they are not treaties drafted with the constitutional assent of the Senate.[89] Hence, ensuring compliance will be a task for these states. For instance, two years after the Xi-Obama Agreement, three Chinese individuals from a Chinese cyber-security firm were caught hacking into the computer systems of a few U.S. companies for commercial gain.[90] Therefore,

[85]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, last visited Oct. 2, 2017; Buchan, R.J. *The International Legal Regulation of Cyber Espionage: Legal, Policy and Industry Perspectives*, NATO CCD COE PUBLICATIONS, Tallinn, 65-86, http://eprints.whiterose.ac.uk/98791/10/Russell_The%20International%20Legal%20Regulation%20of%20Cyber%20Espionage%20_comments%20combined.pdf, (last visited Feb. 18, 2018).

[86]Martin Libicki , *The Coming of Cyber Espionage Norms*, NATO CCD COE PUBLICATION, Tallinn 1, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espionage%20Norms.pdf, (last visited Feb. 20, 2018).

[87]*Id.*

[88]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[89]Matthew Dahl, *Agreements on Commercial Cyber Espionage: An Emerging Norm?*, LAWFARE, December 4, 2015, https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm, (last visited Oct. 2, 2017).

[90]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017,

entering into commercial cyber espionage agreements does not solve the problem for states.

It also depends on the drafting of the agreement. The Xi-Obama agreement was criticized for the specificity of the agreement[91] the loopholes of which can be interpreted to one's advantage. This is similar to how China, through its national security defense to the recent cyber-attack, took advantage of the loopholes in the Xi-Obama Agreement.[92] In case a state seeks to enter into commercial cyber espionage agreements in the future, the parties should clearly lay down the activities that constitute a violation and those that do not. In the absence of such clarity, such agreements would not serve the purpose.

An alternative to tackle this issue is by expanding the application of TRIPS Agreement to specifically address cyber espionage for trade and commercial purposes. This would involve detailed discussions of all the WTO members to find solutions to the above discussed problems in the TRIPS Agreement as it exists currently (such as territorial limitation under National Treatment principle, ambiguity over whether commercial cyber espionage constitutes breach of confidence, etc).

Another avenue could be to pursue a general diplomatic conference outside WTO to address a wide range of issues with respect to cyber espionage including trade and commercial aspects. Such a conference

https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

[91]James Andrew Lewis, *The US Really Does Want to Constrain Commercial Espionage: Why does Nobody Believe It?*, LAWFARE, July 1, 2016, https://www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it, (last visited Oct. 2, 2017).

[92]Jack Goldsmith and Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, LAWFARE, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage, (last visited Feb. 18, 2018).

would be similar to the naval disarmament conferences during the inter-war period where members of the League of Nations took an initiative to actualize the ideology of disarmament.[93] Until the time such an activity is undertaken, there seems very little success of adjudicating a commercial cyber espionage issue at the WTO.

[93]Stuart Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance*, 58 Virginia Lawyer 28 (Feb. 2010).

DATA PROTECTION – PROTECTION OF WHAT, PROTECTION FROM WHOM & PROTECTION FOR WHOM - AN ANALYSIS OF THE LEGAL AND JUDICIAL PROVISIONS IN INDIA AND ABROAD

*Shatakshi Singh**

Abstract

Governments around the world today find themselves shouldered with the dual responsibility of managing economies oiled by data and protecting individual privacy. Such a dichotomous situation begs clarity on three aspects of an effective data protection regime- protection of what, from whom and for whom. These three questions have today emerged as the most pensive issues regarding data protection that policymakers and interpreters around the world are faced with. The article seeks to answer these three questions drawing from the experiences of three parts of the world- the United States of America, the European Union and India. The article, after briefly introducing the concept and need of a data protection regime, discusses in some length the evolution of the right to privacy in India through an analysis of the judicial discourse on the same. Hereinafter, each of the three questions has been discussed in detail under three headers- each header

dealing with one of the three jurisdictions. Answers to the three questions, in context of the three countries under study, shed light on the three aspects of an effective data protection regime- personal data, data subject and data controller. The subsequent section builds upon the answers thus obtained to present a scheme of standards that have gained repute and accolade at the international level and use the same as a benchmark to critically analyse the current nuances of the data protection laws in India. The concluding section of the article indicates the need for a consolidated data protection regime in the country while discussing the recent developments towards the same which is taking shape in the form of the data protection bill.

I. INTRODUCTION AND OVERVIEW

A. The need to protect data- the beginning of a consciousness

With the advent of information technology and large-scale data transfer, there is a growing concern about the whereabouts and safety of personal data. The challenges that are faced with regard to protection and security of data have been recognized today on an international level.[1] From the early 1970s, a large amount of personal

*Shatakshi Singh is a fourth year student at Symbiosis Law School, Noida. The author may be reached at shatakshisingh1996@gmail.com.

[1]*See* Organisation of Economic Cooperation and Development [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, C(80)58/FINAL (July 11 2013), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [hereinafter OECD Guidelines] ; G.A. Res. 217 (iii) A,

information was being processed with the use of computers.[2] This also was the time when the European Economic Community saw a boom in trans-border trade which led to sharing of personal information across borders. This burgeoning data synergy was greatly supported by the advent of the era of information technology.

At this point, it is imperative to understand the meaning of the term Data. The term is defined in section 2(o) of the Information Technology Act, 2000 as follows-[3]

> *"(o) 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."*

The need to protect this data was not always felt in India. The realization that data can be construed as an asset linked to privacy that can ultimately be breached, mainly set in after the expansion of the trend of off- shoring business operations conducted in India.[4] However, when one talks about protecting data, one of the most important things is to ensure that the dual purpose of protection of

Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948); Council of Europe, Convention on the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, ETS No. 005 [hereinafter European Convention on Human Rights].

[2]Sian Rudgard, *Origins and Historical Context of Data Protection Laws*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, (Sept. 23, 1980), https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

[3]The Information Technology Act, 2000, § 2, No. 2, Acts of Parliament, 2000 (India).

[4]*See* Latha R. Nair, *Data Protection Efforts in India: Blind Leading the Blind*, 4 Indian J.L. & Tech. 19, 20 (2008).

privacy and free flow of data is achieved.[5] This kind of dual approach is quite evident in the European Data Protection Directive.[6]

In the Indian context, the framework for data protection is neither structured nor comprehensive. Rather, it is scattered across diverse legislations and constitutional decisions. However, much can be learnt about the data protection jurisprudence of the country by analysing the ultimate source of all data protection laws- the right to privacy. One of the earliest and most authoritative discourses on what constitutes 'right to privacy' can be obtained from the article written by Warren and Brandis in 1890.[7] The article pointed out that the common law, as was in existence then, was insufficient to protect individuals against breach of their privacy rights. They went on to assert that be it tort law, contract law or copyright laws, they all provide a limited and tailored protection against disclosure of personal data and that common law itself contained a more potent tool to protect the right- a tool that was yet to be interpreted. This tool was based on the right to be let alone. The right, as the authors argued was not a property right, rather it stemmed from the idea of "inviolate personality".

The discussion on privacy becomes important since right to privacy is the channel through which an individual can assert the right to control and monitor their personal information.[8] Hence, the right to protect personal information can be very well understood as a component of one's right to privacy. Apart from the statutory provisions, most of the judicial discourse available on data protection stem from one or the other interpretation of the right to privacy.[9] Not only the Indian

[5]*Id.*
[6]Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[7]Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193 (1890).
[8]Glancy Dorothy, *Invention of the Right to Privacy*, 21 Ariz. L. Rev. 1, 40 (1979).
[9]*See infra,* note 18.

judiciary but courts in United States have also recognized the link between data protection laws and right to privacy.[10]

The international recognition of the link between the two kinds of rights is also evident from the European Union Charter of Fundamental Rights. Articles 7 and 8 of the charter talk about "respect for private and family life" and "protection of personal space".[11]

B. Development of Judicial Underpinnings of the Data Protection Discourse in India

The case of *Kharak Singh* v. *State of U.P.*[12] was one of the earliest decisions to deny the right to privacy the status of a fundamental right, though not in very clear terms. However, whether right to privacy can flow from the article 21 of the Constitution and be hence considered a fundamental right has long been a matter of debate owing to the different interpretations adopted by the Supreme Court in different cases.[13]

[10]*United States Dep't of Justice* v. *Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) (holding that one of the essential aspects of privacy is the ability to exercise control over one's personal information).

[11]Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1.

[12]Kharak Singh v. State of U.P. 1963 AIR 1295 (holding that privacy is an essential ingredient of personal liberty under article 21 of the constitution of India).

[13]*See* Unni Krishna, I.P. & Ors. v. State of Andhra Pradesh (1993) AIR 2178; R. Rajagopal & Anr.v. State of Tamil Nadu and Ors. (1994) 6 SCC 632; Peoples Union of Civil Liberties (PUCL) v. Union of India & Anr. (1977) 1 SCC 301 (holding that the right to privacy flows directly from the right to right guaranteed under article 21 of the Indian Constitution). *See*, e.g., M.P. Sharma & Ors. v. Satish Chandra &Ors. AIR 1954 SC 300 (six judge bench held that right to privacy is not a guaranteed right under the constitution).

It has been pointed out by commentators[14] that the turning point in providing constitutional recognition to the right to privacy is the judgment of the Supreme Court in the case of *Gobind* v. *State of Madhya Pradesh*.[15] Though the court stayed shy of declaring right to privacy a fundamental right, it was nevertheless opined by the court that right to privacy found place in the penumbral zone associated with fundamental rights.

Justice Mathew explained the need of data privacy laws in a world where technology was taking personal data into uncharted territory.[16] In later judgments of the Supreme Court, though privacy was again not given an express status of a fundamental right, several components of privacy were sought to be given individual recognition. Hence, in *PUCL* v. *Union of India*,[17] Supreme Court held that unauthorized phone tapping abridged the right to privacy.

Then, in the year 2015 the Supreme Court of India, in the case of *K.S. Puttaswamy and Ors*. v. *Union of India and Ors*[18] held that the diverging opinions of the Supreme Court across different judgments on the right to privacy create a pertinent and pervasive question that must be answered by a nine-judge bench. On 24th February, 2017 the nine judge bench of the Supreme Court declared the right to privacy a fundamental right under article 21 of the constitution of India.[19] In doing so, the judgments in *M.P. Sharma* case and *Kharak Singh* case stand overruled.

[14]Lawrence Liang, *A Right for the Future*, The Hindu (Aug 29, 2017, 12:15 a.m.), http://www.thehindu.com/opinion/lead/a-right-for-the-future/article19576761.ece.
[15]Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
[16]*Id*. ("Time works changes and brings into existence new conditions. Subtler and far reaching means of invading privacy will make it possible to be heard in the street what is whispered in the closet").
[17]PUCL v. Union of India (1996) 2 SCC 752 (holding that right to privacy could not be considered a fundamental right).
[18]K.S. Puttaswamy and Ors. v. Union of India and Ors (2015) 8 SCC 632.
[19]K.S. Puttaswamy and Ors. v. Union of India and Ors (2017) SCC OnLine SC 996.

C. Impact of the Puttaswamy Judgment (2017) On Data Protection in India

By giving the right to privacy a constitutional status, the judgment has laid down the constitutional edifice for a data protection regime.[20] Justice Chandrachur has pointed out the need to balance the protection of sensitive personal data against national security.[21] The judgment lays down some broad rubrics for the data protection regime without actually directing the legislature to frame rules for the same. The judgment will also have a far reaching consequences on the fate of the challenge to the Aadhar Act before a five judge bench of the Supreme Court.[22] Clearly, the judgment will provide impetus to the legislature to pass a comprehensive law on the subject of data protection thereby bringing the data protection regime in India, in line with that of Europe and U.S.A.

The *Puttuswamy* judgement, in more ways than one has transformed the way in which a common man views the right to privacy. By making informational privacy a part of the broader right to privacy,[23] the judgement has provided a jurisprudential backing to the coveted data protection regime that has oft been ignored while interpreting the constitutional right to privacy.[24] The judgement has laid the foundation on which the legislature, by means of a data protection act, can legitimately indulge in a balancing act between the interests of the individual and needs of the state with respect to protection of personal

[20]Agnidipto Tarafder And Arindrajit Basu, *For the Many and the Few: What a Fundamental Right to Privacy Means for India*, The Wire (Aug 25, 2017, 12:00 a.m.), https://thewire.in/170988/right-to-privacy-supreme-court-2/.
[21]Puttuswamy, *supra* note 18 at ¶ 179.
[22]*Id.*
[23]*Id.* at ¶ 177.
[24]Live Law Staff, *This Is What Supreme Court Said In Right To Privacy Judgment*, Live Law (Aug 24, 2017, 12:00 a.m.), http://www.livelaw.in/supreme-court-said-right-privacy-judgment-read-judgment/.

information. The concluding section of the paper will build upon the discourse that has been created by the judgement.

II. PROTECTION OF WHAT

In this nascent stage of information technology, data protection laws have been hailed as a novel area of law.[25] As has been already specified in the beginning of this paper, 'data' in the present study refers to personal data. However, the ambit of personal data is not easy to define. It can assume different forms in different places over different periods of time. Hence, it is important to understand what exactly data protection laws across the globe seek to protect.

Labelled as the "currency" of digital economy, protection of personal data has assumed great importance in this electronically interconnected globalised world.[26] Across most of the definitions of personal data, it is recognised that personal data has the capability to 'identify' an individual.[27] If personal data can be considered the currency of the digital economy then big data can be definitely referred to as a jackpot.[28] In the simplest terms big data is an uncontrolled explosion of digital data- a kind of situation where the 'management' of the bulk of data becomes impossible because of lack

[25]Stephanie J. Frazee, *Bloggers as reporters: An Effect Based Approach to First Amendment protections in a New Age of Information Dissemination*, 8 Vand. J. Ent. & Tech. L. 609, 640 (2006).
[26]Diane A. MacDonald, Christine M. Streatfield, *Personal Data Privacy And The WTO*, 36 Hous. J. Int'l L. 625, 626 (2014).
[27]*Id.*
[28]JAMES MANYIKA ET AL., *BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY, (*McKinsey Global Inst. ed.,2011) (Defining Big Data as data bases that are too mammoth in size to be handled by typical database software tools to manage, analyse capture and store).

of tools to 'measure' it[29].Many have pointed out that big data leads to development of transformative innovation. However, the downside of the story reveals the potent threat that personal data can pose when stored and transmitted around the world in the form of big data.

It should be further noted that personal data can refer to personal as well as commercial aspects of information. Though both fall within the ambit of personal data, they produce different results when breached. Protection of personal aspects of information falls within ambit of privacy rights while protection of commercial aspects falls in the realm of proprietary rights. Hence, data protection entails both privacy as well as proprietary rights.

Given the different interpretations that can be accorded to the term personal data, it is important to understand the scope and ambit of the term across various legislations around the world.

A. Position in the U.S.A

The U.S.A. has a sectoral data protection law. This is because the laws are fragmented and spread across governmental and industry specific regulations. The U.S.A does not recognize a fundamental right to privacy.[30] Nor does the constitution in the U.S.A accord direct protection to the right to privacy. Nevertheless, the right can be implicitly derived from the First, Third, Fourth, Fifth, and Fourteenth amendment.[31]

[29]Andrew McAfee, Erik Brynjolfsson, *Big Data: The Management Revolution*, Harvard Business Review (Oct, 2012), https://hbr.org/2012/10/big-data-the-management-revolution.

[30]*See* Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I- The Current Impact of Surveillance on Privacy*, 66 Colum. L. Rev. 1003, 1032 (1966) (noting that the right to privacy can be compromised on the altar of general public welfare).

[31]*See* U.S. Const. amends. I, III, IV, V, XIV; Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965); Roe v. Wade, 410 U.S. 113, 153 (1973).

To address the question of what U.S.A.'s data protection laws protect, it is observed that the industries which contain data protection laws are those which handle or transmit sensitive personal information. Before discussing in detail the ambit of personal data it is imperative to first list some of the most important Federal laws on Data protection that exist in the U.S.-

- Federal Trade Commission Act-[32] it is a consumer protection law that seeks to curb the deceptive trade practices and has been also extended to the offline and online privacy and data security policies. The companies that fail to comply with posted privacy policies face enforcement actions under the act for the disclosure of personal data.[33]

- The Financial Services Modernisation Act-[34] it regulates the use, disclosure and collection of financial information.[35]

- The Health Insurance Portability and Accountability Act ["HIPAA"]-[36] it is a provision to regulate the medical information and can apply to data processors, health care providers, pharmacies and other entities.[37]

- The Electronic Communications Privacy[38] Act and The Computer Fraud and Abuse Act[39]- while the former

[32]Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1914).
[33]Leuan Jolly, *Data Protection in The United States: Overview*, Thomson Reuters (Jul 1, 2017), https://uk.practicallaw.thomsonreuters.com/6-502 467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.
[34]Financial Services Modernisation Act, 15 U.S.C §§ 6801- 6827 (1999).
[35]*Supra* note 21.
[36]The Health Insurance Portability and Accountability Act, 42 U.S.C et sq. (1996).
[37]*Supra* note 21.
[38]Electronic Communications Privacy, 18 U.S.C § 2510 (1986).
[39]The Computer Fraud and Abuse Act, 18 U.S.C §1030 (1984).

> protects the interception of electronic communication, the latter regulates the tampering of computer resources.

Apart from the above federal laws, there exist several state laws as well that protect personal data. California is the leader in this field and has enacted several personal data privacy laws whose importance resonates even at the national level.[40]

Now it is essential to come to the main question in discussion under this section- i.e. "What data is regulated?" Much like the nature of the data protection laws available across the United States, the answer to this question is also scattered and fragmented and depends on the law under consideration. For example, the FTC Act does not explicitly mention the category of data that it seeks to protect. What it prohibits are such practices that can potentially render the personal information of consumers at the risk of exploitation and hacking.[41] Such personal information would include consumers' searches online, the web pages visited, the contents viewed etc.

The FSM Act regulates the personal information that is collected from consumers who avail financial services and products for commercial or non- commercial purposes from a financial institution.[42] Hence, the personal information here mainly refers to the financial personal information of the consumer.

[40]The law in California mandates a state body or a business entity to send due notice to any resident of California in case his/her unencrypted personal information has been acquired or is reasonably believed to have been acquired, *see* California Civ. Code, § 1798.29(a)(1977) (for state bodies); California Civ. Code, § 1798.82(A) (1977) (for businesses).

[41]Federal Trade Commission Act, 15 U.S.C. § 45b(b)2 (1914).

[42]*See* Financial Services Modernisation Act, 15 U.S.C § 6802 (1999).

Similarly, within the purview of HIPAA, personal information would mean individually identifiable health and medical information.[43]

Again, as per California Security Breach Notification Law, any individual's first name or first initials and last name together with social security no., Driver's License, Account No., Credit or debit Card No, Medical Information or Health Insurance Information would constitute personal information.[44] Hence, it can be seen that the thrust is on that combination of information that can potently identify an individual.

It has been noted that in the United States, the definition of "personal information" remains uncertain.[45] While certain legislations like the Electronic Communication Privacy Act[46] seek to protect the personal information of individuals in transitory, final or stored communication (wire, oral and electronic communication), others like the Computer Fraud and Abuse Act[47] protect a wide variety of personal information including defence related information, financial transaction data etc. In fact, legislations like the Children's Online Privacy Protection act[48] and Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records[49] employ particularly circular definitions of personal data. While the former defines personal data as the data which provides individually identifiable information about an individual, the latter defines personal data as that data which identifies an individual. Clearly this

[43]The Health Insurance Portability and Accountability Act, 42 U.S.A §1301 et sq. (1996).
[44]*Supra* note 40.
[45]*See* McKay Cunningham, *Complying With International Data Protection Law*, 84 U. Cin. L. Rev. 421, 425 (2016)
[46]Electronic Communication Privacy Act, 18 U.S.C. § 2510-22 (1986).
[47]Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
[48]Children's Online Privacy Protection Act, 15 U.S.C § 6501(8).
[49]Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records, 18 U.S.C § 2725 (2000).

lack of consistency has led to widespread regulatory uncertainty and discord.

B. Position in the E.U.

Privacy has been declared a fundamental right in the E.U.[50] Unlike the sectoral approach to Data Protection legislation adopted in the U.S.A, the E.U., for the purpose of regulating the use and transfer of personal data, enacted a common legislation.[51] Under this legislation the term personal data has been defined as follows-

> *"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 byreference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."*[52]

The above definition is wider than the U.S definitions. Under the EU legislation whenever someone links a certain piece of information to a specific person, that information will be considered personal, even if the link is not apparent to the person holding the information. [53] This can be understood in light of the fact that even IP addresses and cookies have been recognised as personal data by The Working Party on Data Privacy.[54] Some entities try to evade the data privacy laws by

[50]*See* Pamela Samuelason, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1134 (2000).
[51]Council Directive 95/46/EC, *supra* note 6, arts. 5-6 [henceforth EU Directive].
[52]*Id*. art. 2(a).
[53]*See* OAUL m. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U.L. Rev. 1814, 1819 (2011).
[54]Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search engines*, E.U., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

making the information anonymous.[55] Since such data cannot be identified with any particular individual the attempt is to take it effectively outside the ambit of personal data. However, it has been recently brought to light that even anonymous data can reveal information through carefully coded algorithmic scripts.[56]

Hence, the EU Directives'[57] definition of what is personal data is far more ambitious and multifaceted than the definitions prevalent in the U.S.A. The consolidated nature of the law in form of the directive[58] gives coherence and structure to the ambit of Personal Data and hence facilitates efficient implementation of Data Protection norms. This efficiency arises from the lack of ambiguity about whether a certain piece of information would qualify as 'personal' or not. The directive, by including data which indirectly identifies an individual within the ambit of personal data, has accorded greater protection to the identity of an individual. Here, it is imperative to mention that on 25 May, 2016 the EU General Data Protection Regulations[59] were adopted after a number of deliberations. By 25 May, 2018 the new regulations shall replace the current Directive (EU 95/46/EC). In broad terms, the GDPR defines personal Data as any information that can be directly or indirectly used to identify a natural person. It can include anything from the email address, bank details till the photo of the individual.[60]

[55]*See* Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J. Of Law and Tech 1 (2011).
[56]Arvind Narayan, Vitaly Shmatikov, *Myths and Fallacies of 'Personally Identifiable Information'*, Communications Of The Acm, (Jan 27, 2011), https://cacm.acm.org/.../2010/...myths-and-fallacies-of-personally-identifiable-inform.
[57]EU Directive.
[58]*Id.*
[59]Council Regulation 2016/679 of Apr. 27 2017 on The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter EU GDPR].
[60]Sivarama Krishna et al., *Demystifying the EU General Data Protection Regulation*, PwC, (Sept, 2016), http://www.pwc.in/assets/pdfs/consulting/cyber-security/demystifying-the-eu-general-data-protection-regulation.pdf.

It is to be noted here that unlike the old directive, where the member states of EU were required to come up with their own legislations on data protection (within the wide ambit of the directive), the new GDPR seeks to create uniformity in the substantive part of the data protection regulation.[61] It envisages a transfer of power in the hands of the individual to exercise control over the processing of their personal data.[62] By including 'biometric' and 'genetic information' within the ambit of personal data, the GDPR will go a long way in ensuring that every aspect of personal information is protected.[63]

C. Position in India

India neither has consolidated data protection laws such as the EU, nor does it have sectoral laws such as exist in the U.S.A. However, this does not imply an absolute absence of legal protection in this regard. As already discussed, there exists in India, a rich stock of judicial decisions on the right to privacy which have been construed as giving way to the right to protection of personal data. Other than such jurisprudence, data protections norms can be culled out from The Indian Contract Act, 1872,[64] The Information Technology Act, 2000,[65] The Information technology (Amendment) Act 2008 and the 2011 rules implementing some of the provisions of the IT amendment act, 2008.[66] Other than the above provisions, the use of financial information is regulated by The Credit Information Companies

[61]However, some room will be provided for the individual states to legislate on the procedural aspects of the legislation, *see* Aditi Chaturvedi, *Comparison of General Data Protection Regulation and Data Protection Directive,*The Centre For Internet & Society (Feb 7, 2017), https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive.
[62]*Id.*
[63]*Id.*
[64]The Indian Contract Act, 1860, No. 9, Acts of Parliament, 1872 (India).
[65]*Supra* note 3.
[66]Notification no. G.S.R. 313(E), April 11, 2011, Extraordinary, Part 2, § 3(i), Gazette of India.

(Regulation) Act, 2005[67] and to a certain extent by The Prevention of Money Laundering Act, 2002.[68]

As per the 2011 rules, personal information has been defined as information which in combination with some other information available or likely to be available with a body corporate relates to the identity of an individual either directly or indirectly.[69] The rules however mark a separate category or subset of personal information in the form of Sensitive Personal Information.[70] Any personal information that relates to the following is termed as sensitive data-

a) Passwords
b) Financial information
c) Physical, psychological and mental health condition
d) Sexual orientation
e) Medical records and history
f) Biometric information
g) Any information from (a)-(f) received by a body corporate for provision of services; or
h) Any information relating to (a)-(g) that is received, stored or processed by the body corporate under a lawful contract or otherwise.

It is to be further noted that information available under the Right to Information Act 2005[71] is exempt from the above two definitions.[72] Certain other classes of information like religious beliefs, ethnicity and political opinions are also not covered under definition of

[67]The Credit Information Companies (Regulation) Act, No. 30, Acts of Parliament, 2005, (India).
[68]The Prevention of Money Laundering Act, No. 15, Acts of Parliament, 2003, (India).
[69]*Id*. at Rule 2(i)
[70]*Id*. at Rule 3.
[71]Right to Information Act, No. 22, Acts of Parliament 2005 (India).
[72]*Id.*

sensitive information. Such information does find mention in the sensitive personal information category in other jurisdictions either.[73]

Under the CIC Act, personal information entails all the information that needs to be necessarily furnished by the customer to establish his/her identity.[74] The CIC regime accordingly mandates the CICs, Credit Institutions and the others to establish concrete principles for the collection and use of such personal information.

Here it is to be noted that the draft Personal Data protection Bill 2006 introduced in Parliament on 18th October 2010 lapsed without being realised into a law.[75] Further in 2011 and 2014 a non-profit organization called Centre for Internet and Society released draft privacy Bills on the Internet that recognized individual's right to privacy but allowed invasion of the same for some larger considerations.[76] Further, in May 2016 it was asserted by the Minister for Communication and Information Technology Mr. Ravishankar Prasad that the government was still working on the proposed law.[77] It should be noted that the draft of the proposed privacy bill defines personal data as[78] data which relates to a living, natural person if that person can be identified from that data in conjunction with other data the controller has or is likely to have.

[73]Sreenidhi Srinivasan, Namrata Mukherjee, *Building an Effective Data Protection Regime*, Vidhi Centre For Legal Policy (Jan, 2017), http://vidhilegalpolicy.in/public-law/.
[74]The Credit Information Companies (Regulation) Act, §§ 14 & 17, No. 30, Acts of Parliament, 2005, (India).
[75]Raghunath Ananthapur, *India's new Data Protection Legislation*, 8 SCRIPTED 192, 2013 (2011).
[76]Aditi Subramaniam, *The Privacy, Data Protection and Cybersecurity Law Review*, The Law Review (Nov, 2016), http://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-3/1140175/india.
[77]*Id.*
[78]Hari Subramaniam, Data Protection 2017, ICLG, (May 15, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/india.

Further, the sensitive personal information has been defined by the bill as relating to unique identifiers such as-[79]

a) Aadhar number or PAN;
b) Physical and mental health;
c) Biometric or genetic information
d) Banking credit and financial data; and
e) Narco Analysis and /or Polygraph test data.

Hence, it is clear that legislation in India is diverse on the issue of ambit of personal data. A comparison between the three countries reveals that India needs to adopt a broad umbrella legislation with an expansive definition of 'personal data' on the lines of the EU laws. The EU directive states that all data with which an individual can be identified or is identifiable, should fall within the ambit of personal data. Following from this, the definition of personal data in India must not be myopic so as to be limited only to that information which directly relates to an individual. Since the IT Act and Rules prescribe the ambit of personal data in the form of pointers referring to a certain type of personal information, it should be replaced with a more general approach like that of EU wherein any information is construed as personal information if it either directly or indirectly leads to the identity of an individual.

Also, unlike in the U.S.A, India should not experiment with sectoral definitions of personal data. A scattered definition would add to the entropy that already exists in India due to the absence of a comprehensive data protection regime.

[79] *Id.*

III. PROTECTION FROM WHOM

The next question to be addressed is against whom should such protection be sought. In modern democracies, there has been an upsurge in cross border data trade. With data being collected and transferred not just by the government but also, at a faster pace, by the private sector.[80]

With respect to the government, its desire to accumulate more and more personal data about its subjects has grown over the past decade. This increase in appetite for personal data of individuals stems from a new model of administration that governments across the globe seem to have adopted- 'data processing model of administrative control'.[81] Personal data is being collected for a variety of purposes like taxation, issuance of license, voter registration, employee identity verification, law enforcement etc. The new threats to national security in the form of terrorist attacks has added further impetus for the government to seek personal data of every individual who goes in and out of the country.[82] It is to be noted however, that though the need/desire on part of government to collect personal information has existed for a long time, the accessibility to the same has considerably increased over the past decade.[83] This has mainly happened due to two reasons-

The *first* relates to the sharp increase in the amount of data being generated and transmitted from within the country to other countries. Hence, information related people's lives in the industrialised world is increasingly available in other countries. The *second* reason stems

[80]Shrishti Saxena, *Data Protection in India*, LIVE LAW (May 15, 2017), http://www.livelaw.in/data-protection-india/.
[81]Paul Schwartz, *Data Processing and the Government Administration*: *The Failure of the American Legal Response to the Computer*, 43 Hatings Law J., 1321, 1326 (1992).
[82]*Id.*
[83]*Id.*

from the fact that government can today easily access personal data of its subjects from third party sources.[84]

Considering these factors, the attempt will now be to analyse the situation in the United States, the E.U., and India to determine against which entity the data protection laws of these jurisdictions seek to accord protection. The answer to this question will in a large way affect the future of data privacy across a world where the demarcation between public and private is fast waning.

A. Position in the U.S.

As already discussed, the data protections laws in the U.S.A are highly sectoral and unlike the E.U. there is no comprehensive legislation on the same. This peculiar nature of the data protection laws makes it difficult to clearly pinpoint the exact authorities against which the laws seek to accord protection. However, it can be generally stated that the federal laws seek to regularize the collection and dissemination of personal data by "consumer reporting agencies",[85] oversee the collection and handling of personal data by federal governmental agencies,[86] and mandate financial service corporations to adopt such measures as would ensure the privacy and safety of consumer's personal data. [87] Hence, despite being very diversified, the data protection laws are pitched to provide protection against both the public and the private sector.

However, it is essential to understand that the data protection jurisprudence that developed in the U.S. was the result of inherent and

[84]Fred H. Cate, James X. Dempsey, and Ira S. Rubinstein, *Systematic Government Access to Private Sector*, International Data Privacy Law (Sept. 17, 2012), https://oup.silverchair-cdn.com/oup/backfile/Content_public/Journal/idpl/2/4/10.1093/idpl/ips027/2/ips027.pdf.
[85]Fair Credit Reporting Act, 15 U.S.C. § 1681 (West 2014).
[86]Privacy Act of 1974, U.S.C. § 552a (West 2014).
[87]Gramm- Leach Bliley Act, 15 U.S.C. §§ 6801- 6809 (West 2011).

inborn suspicion in the minds of the citizens regarding the misuse of state power.[88] This can be seen in light of the fact that modern laws on data protection can trace their origin to the Bill of Rights which sought to impose restrictions on State power.[89] In modern times, in fact, the data protection laws stem from the recognition that was accorded to privacy by US Courts under the Fourth Amendment.[90]

Apart from the data protection legislations that accord protection to the American citizenry against both private and governmental encroachment on personal data, a rich judicial discourse further strengthens this protection against the government and it agencies, through a string of case laws. In one of the much-acclaimed articles by Samuel Warren and Louis Brandeis it has been asserted that the best way to protect personal data is by keeping it outside the public domain.[91]

Though protection to personal data has been provided against both the government and the private sector, the multitude of the legislations has left much task of interpretation in the hands of the judiciary. Hence a trend has emerged to the effect that in most of the complaints regarding data breaches, either against the government or the private

[88]*See* James Q. Whitman, *The Two Western Cultures of Privacy: Digital Versus Liberty*, 113 Yale L.J. 1151, 1153 (2004).
[89]*Id.* at 1211-12.
[90]*See* City of Ontario v. Quon, 560 U.S. 746, 755-56 (2010) (Holding that the Fourth Amendment guarantees that the invasive and encroaching acts of officers of government does not evade privacy, dignity and security if citizens); Olmstead v. United States, 277 U.S. 438,478 (1928) (Holding that the citizen in the U.S. had the right of be left alone against the government and that the framers of the U.S. constitution had sought to protect the citizens in their beliefs, thoughts, emotions and sensations).
[91]Samuel Warren, Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1980).

sector, the judiciary demarcates the limits of data protection on a case to case basis.[92]

B. Position in Europe

Europe, unlike U.S.A has a very comprehensive and well defined system of data protection laws that recognises right to privacy as a fundamental right.[93] Considering the technological boom in the 1960s, and the rapid use of computers for storing citizens' personal data *en masse*, a need was felt to accord protection against both private entities and the government.[94] Accordingly, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was presented by the Council of Europe for adoption by the European Nations. It came to be known as Convention 108 and is the only legally binding instrument that exists in the area of Data Protection. [95]The most striking feature of the Convention is that it equally applies to public and private entities as long as they are involved in collecting personal data.[96]

Following this, on October 24, 1995 Directive 95/46/EC was issued by the Council of Europe and the European Parliament on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data." [97] Even though the members of EU have already integrated the principles of Convention 108 in their national laws, a need was felt to have a comprehensive

[92]Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn. St L. Rev. 587, 600 (2007).
[93]Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14 art. 8(1), Nov 4, 1950, ETS No. 5.
[94]Christina Glon, *Data Protection in The European Union: Closer Look at the Current Patchwork of Data protection Laws and the Proposed Reforms That Could Replace Them All*, 42 Int'l J. Legal Info. 471, 492 (2014).
[95]COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014).
[96]*Id.*at 62.
[97]*Id*. at 6.

law that would give common cross border definitions of the various aspects of data protection laws.[98]

Another contribution made by the Directive was that it clearly demarcated the ambit of the term controller and processor of personal Data. Under the EU laws a controller is a person who –

> *"Alone or jointly with others determines the purpose and means of the processing of personal data".* [99]

Any entity that can be held responsible under the applicable law and falls within the ambit of the definition of Data Controller shall be considered the same. This means that any natural or legal person in the private sector and any authority in the public sector can be held responsible as a data controller.[100] From here it can be fairly concluded that the Directive applies equally to the private as well as the public sector.

Such a comprehensive coverage ensures a wholesome protection to the personal data of the data subjects such, without any bias towards either the public or the private sector.

Further, in December 2000, The European Council and the European Parliament together passed Regulation (EC) No. 45/2001.[101] This regulation has expanded the scope of Directive 95/45/EC to all 'community institutions and bodies" other than governmental bodies. A European Data Protection Supervisor has been appointed as an independent supervisory entity to ensure proper enforcement of the

[98] *Id.* at 62.
[99] Data Protection Directive, art. 2(d).
[100] *Id*. at 64.
[101] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on The Protection of Individuals With Regard to The Processing of Personal Data by The Community Institutions and Bodies on The Free Movement of Such Data, 2001 O.J. (L 8)1, 3 [hereinafter Regulation (EC) 45/2001].

regulation. This further ensures that a large gamete of public authorities is brought within the ambit of Data Protection laws.

Under the newly formulated EU GDPR,[102] any organization involved in the processing (which included collection and dissemination) of personal data can be divided into two categories- data controller and data processor. The organization that collects personal data from the consumers is called the data controller. The controller has the power to ascertain the manner in which this personal information is to be used.[103] This data controller can further send the personal data to other entities for processing purposes. Hence organizations that are involved in mere storage and processing of the personal data on behalf of the controller are called data processors.[104] Both of these entities would be under the scrutiny of the EU GDPR.

C. Position in India

Despite the lack of a comprehensive framework, there are certain legislations that cover the aspect of data protection and provide some relief, howsoever limited, in the area. Apart from these legislations, the courts in India have played an active role in developing the culture of data protection by giving an expansive definition to the Right to Privacy.

When it comes to statutory provisions, the most important and comprehensive one on the issue of data protection is the Information and Technology Act, 2000, amended by the Information Technology Amendment Act (2008).[105] This act provides for civil prosecution[106] in the case of "Cyber contraventions" and criminal action[107] in the

[102]EU GDPR.
[103]*Supra* note 39.
[104]*Id.*
[105]The Information Technology Act, 2000, No. 2, § 2, Acts of Parliament, 2000 (India).
[106]*Id*. at § 43(a)-(h).
[107]*Id.* at §§ 63-74.

case of "cyber offences". The main question under this section, however, is to understand the entities against which the laws in India seek to accord protection. The IT Act as amended in 2008 provides that-

> *"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."*[108]

Hence the act provides protection to sensitive personal data against body corporate, i.e., companies, sole proprietorships or associations that collect or process sensitive personal data.[109] It is to be noted that the provision nowhere mentions any public authority and refers to only corporate entities. Even if one were to resort to section 72A one would find that it protects the contractual obligation between a company and its customer in relation to disclosure of sensitive personal information. However, it is to be noted that unlike section 72 of the IT Act 2000 which was limited to authorities and service providers, section 72 A provides protection against any person who handles personal data under the terms of a lawful contract. However, neither of the above sections provide any effective protection of data against government entities.[110] The fact that public authorities are excluded from the ambit of the major provisions relating to data protection, seriously limits the scope of the law. Even the IT Rules of

[108] *Id.* at §43 A.
[109] Asang Wankhede, *Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data*, 2 Eur. Data Prot. L. Rev. 70, 79 (2016).
[110] *Id.*

2011 provide extensive rules for data protection only against the corporate entities.[111]

On an analysis of the above jurisdictions and on the basis of discussion in an earlier section, it can be fairly concluded that just like the U.S., the Indian judiciary has played an important role in evolving the data protection jurisprudence. The U.S. however, protects the privacy right of individuals through judicial discourse as well as legislation- wherein the legislation accords protection against the private entities as well as the state. In India on the other hand, the entire legal framework provides protection only against the activities of private bodies. The judiciary, through expansive interpretations of the right to privacy has indeed heralded a new chapter in data protection against the government, but much needs to be done in terms of legislation to bring government and related entities within the ambit of privacy laws. Like the U.S the EU also accords protection against both the public as well as private sector but unlike the U.S the EU provides this wholesome protection under an umbrella law. Hence it can be seen that just like the previous section on 'protection of what', it can be fairly concluded that India needs a unified data protection regime which accords protection against the private sector as well as government entities.

IV. PROTECTION FOR WHOM

The concern over the protection of personal information has become a widespread phenomenon across the globe. People today, more than

[111]Hari Subramaniam, Aditi Subramaniam, *Data protection 2017*, ICLG, (15 May, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/india.

ever before are concerned about the threats posed to data privacy from the public as well as the private sector.[112]

Across all the geographical areas in consideration, i.e., U.S, E.U. and India, the cynosure of the provisions relating to data protection is the individual. Per the E.U. Data Protection Directive[113] Data Subject is –

> *"Any identifiable or identified natural person- meaning thereby who can be identified directly or indirectly.*[114]

In fact, some countries have left the definition of "data subject" totally outside the purview of any statute. An example on point is the U.S. wherein none of the statutes define the "data subject".[115]

Coming to the Indian context, it has been pointed out, that with reference to the IT Rules 2011[116], the distinction between "the provider of information" and the person "to whom the data pertains" i.e. the Data Subject can cause lot of confusion in terms of defining the rights of the individual whose identity can potentially be disclosed by the personal information.[117]

[112]David Banisar, Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Development*, 18 J. Marshall J. Computer & Info. L. 1, 3 (1999).
[113]Council Directive 95/46, 1995 O.J. (L281) 31 (EC) ch 1 art. 2(a).
[114]Donald C. Doling, Jr., *International Data Protection Law*, White & Case, (Aug, 2009), https://intellicentrics.ca/wp-content/uploads/dlm_uploads/2014/09/article_intldataprotectionandprivacylaw_v5-1.pdf.
[115]Aaron P. Simpson, Jenna Rode, *Data Protection- 2017 (U.S.A)*, ICLG, (May 15, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/usa.
[116]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R 313(E), Gazette of India, section 3(i)(India).
[117]Radha Raghavan, Ramya Ramchandran, *Data Protection Law in India: An Overview*, LEX- WARRIER, (Jan 29, 2013), http://lex-warrier.in/2013/01/indias-data-protection-law-an-overview/.

V. THE INTERNATIONAL BENCHMARK AND INDIA

After having undertaken a comprehensive analysis of the major components of the data protection laws across three different geographical regions, this section seeks to shed some light on the tenets of Indian Data protection laws (particularly the IT Act, 2008 and the IT Rules 2011) and their international credibility. It is to be noted that the major aspects of the IT Act and the Rules in terms of Data subject, Data Controller and the nature of data have already been discussed in the previous sections. This section aims to elucidate upon the technical aspects of data processing that the law envisages.

India, being one of the most popular outsourcing destinations, witnesses the inflow and outflow of a huge quantity of data across its borders.[118] This large data market requires robust regulatory measures and the same will be discussed in the present section. However, before moving to the Indian scenario it is important to briefly understand the international standards that are expected out of a data protection regime.

A. The International Benchmark for Data Protection

There is no authoritative compilation stating the exact standards that a data protection law is expected to follow. However, there are certain works of authority which give a general idea of the horizons of data protection laws through a set of principles. It is noted by Bennet and Raab that a set of twelve "fair information principles" have been widely acknowledged as covering the major dimensions of fair data protection laws.[119]

[118]Probir Roy Chowdhury, Soumya Patnaik, *Data Protection in India*, TAYLOR WESSING (May, 2015), https://www.taylorwessing.com/globaldatahub/article_dp_cyber_india.html.
[119]Graham Leaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, 23 J.L. Inf. & Sci. 4, 9 (2014).

These principles are- accountability; collection with knowledge; use limited to identified purpose; retention only as long as required; individual correction; data kept accurate; limited collection to where necessary for purpose; purpose identification; security safeguards; openness on policies and practices; individual access and data quality.[120] Hence any data protection regulation should be an international embodiment of these twelve principles tailored as per the national needs.[121]

Other than the above set of principles, several other sets of data protection bench marks are also available.[122] Apart from these, there are certain other international instruments which throw light on the facets of data protection laws.[123] Two of these are the OECD privacy Guidelines of 1981[124] and the Council of Europe (CoE) Data Protection Convention 108 of 1981.[125] If the standards laid down in these two instruments are combined, a comprehensive set of principles concerning data protection can be obtained. The principles can be summarized as follows[126]

Collection of data

- *Data Quality*
- *Collection*
- *Purpose Specification*

Communication to data subject

[120]*Id.*
[121]*Id.*
[122]Some authors have also included 'sensitivity' amongst the important principles that a data protection law is expected to follow, *see* e.g., LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 11-12 (BOOK ED. 2002).
[123]European Convention on Human Rights ETS 5, (Nov. 3, 1950) art. 8(1) (1950).
[124]OECD Guidelines.
[125]ETS No. 108, *supra* note 72.
[126]*See supra* note 98.

- *Uses & disclosures limited to purpose specified or compatible*
- *Openness in personal data practices*
- *Mandatory data sharing*

Notice of purpose and rights at the time of collection-

- *Individual's right to access data*
- *Individual's right to correct data*

Security Measures

- *Security through reasonable safeguards.*
- *Accountability of data controller.*

Having stated the basic principles that data protection laws across the world are expected to follow, it is now essential to analyse in some detail the adherence of the provisions relating to data protection in India, to these standards.

B. Analysing the Data Protection Regime in India

The embodiment of the international standards in data protection laws can be best found in the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (IT Rules).[127]

These rules have attempted to introduce several of the above principles, like purpose specification, consent, collection, limitation etc., in the Indian data protection regime. Section 43A of the IT act[128] which uses the words 'sensitive personal information' and 'reasonable

[127]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R 313(E), Gazette of India, section 3(i)(India) (hereinafter IT Rules).

[128] The Information Technology Act, 2000, No. 2, § 43A, Acts of Parliament, 2000 (India) (hereinafter IT Act).

security practices', reserves the scope of making rules for defining the same.[129]

The scope of the section 43A and the IT Rules have already been discussed in previous sections, however, it is essential here to reiterate that the provisions apply only to 'body corporates' that handle 'personal information' or 'sensitive personal information'.[130] The definition of body corporate as given in section 43A totally excludes government entities and individuals from its purview.

Following are some of the major provisions of the Rules which can be analysed in terms of adherence to the international standards laid down for data protection laws-

a) Consent to the collection of information

To understand the requirement of consent in the collection of information, it will be helpful to peruse into the bare provision which is as follows-

> *"Rule 5. Collection of information- (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information."*[131]

It is to be noted that both the individual and a third party can be the source of personal information about the individual. Rule 5(3) of the IT Rules specify that when the source of collection of personal information is the individual (whose personal information is being collected) himself, the details of the intended recipients, purpose of

[129]Srinivasan, *supra* note 48.
[130]IT Act, § 43A.
[131]Rule 5(1), IT Rules.

collection, contact details of collecting and storing entities etc. should be made known to him.[132]

In cases where the personal information about a person is being obtained from a third party source, all the accompanying rights such as right of access etc., will be available to the third party and not to the data subject. This provision clearly dilutes the requirement of consent of the person to whom the personal data actually pertains.[133]

Moreover, an organization that has collected the personal information cannot disclose the same without the prior permission of the information provider.[134] However, if such disclosure was already permitted in the original contract between data provider and receiver then there is no requirement of prior consent. It is to be noted here that this provision is a variation of the internationally acceptable 'use limitation' principle of data protection laws. [135]

b) Communication of Information to Data Subjects

The important component of this rule lies in the mandatory privacy policy that all organisations dealing with personal information are supposed to have in place. The organizations are further required to make this privacy policy available in public domain so that the providers of information can readily view it. The organizations are expected to publish information about the purpose and usage of data collected, types of data collected, and the reasonable security practices that have been adopted by the organization, etc.[136] This principle is drawn from the 'openness' or 'notice' principle of data

[132]Rule 5(3), IT Rules.
[133]The person to whom the personal data directly pertains is often refered to as the 'Data Subject'; Srinivasan, *supra* note 48.
[134]Rule 6, IT Rules.
[135]OECD GUIDELINES.
[136]Rule 4, IT Rules.

privacy acceptable at the international level.[137] However, the mere fact that an organization has in place an internally developed privacy policy does not absolve it from the other norms that are to be followed under an effective data protection regime.[138]

Apart from the requirement of disclosing the privacy policy, there also exists a notice requirement. Notice pertaining to certain important details like intended recipients, contact details of collecting and storing organizations need to be made known to an individual when data is being collected directly from him.[139] However this information does not include within its ambit, details regarding right to limit use and disclosure, or right to ask for erasure of certain pieces of information.[140] This limits the individual's capability to exercise control over personal data.

c) Mandatory Data Sharing

Whenever sharing of information with the government is mandated under any law, the organizations do not need any consent from the data subjects or the data providers before disclosing personal or even sensitive personal information pertaining to them.[141] The rationale is that the government will always use personal data of people for purposes of maintaining law and order. Such personal information can aid the government to detect, prevent and investigate instances of cyber-crime. However, there is one minor safeguard provided. The government will have to send the request for seeking the personal information in writing to the organization and will have to also specify the purpose of seeking information relating to that particular

[137] *Supra* note 113.
[138] PLANNING COMMISSION OF INDIA, *REPORT OF GROUP OF EXPERTS ON PRIVACY*, (CHAIRED BY JUSTICE A.P SHAH), (2012).
[139] Rule 5(3), IT Rules.
[140] *Id.*
[141] Proviso to Rule 6(1), IT Rules.

individual or group of individuals.[142] The government is also supposed to state that the information so obtained will not be shared with any other person.[143] However, there is no limitation on the period for which the government can hold such information.[144] Also, even after the investigation using the information obtained has come to an end, there is no provision to let the data subject know that personal information relating to him was shared in the first place. The fact that section 43A is entirely focused on the body corporate, again excludes any protection against the government matters of data protection. [145]

d) Right to Access Information

The rules provide that the provider of information (the data subject or the third person provider of information), has the right to review information pertaining to them and ask for corrections in case there are any irregularities.[146] The rules further provide that every organization is supposed to designate one grievance officer who is to take complaints from the providers of information in respect of any discrepancy in information pertaining to them.[147] Such an interface will greatly facilitate increased control of the provider of information on their personal data. Also, the fact that the rules mandate the resolution of the disputes within a month puts the Indian data protection regime a step forward in achieving international standards.[148]

Though the above provision is a positive step towards empowering the data provider (and not necessarily the data subject), it is to be

[142] *Id.*
[143] *Id.*
[144] REPORT OF GROUP OF EXPERTS, *Supra* note 126.
[145] Srinivasan, *supra* note 48.
[146] Rule 5(6), IT Rules.
[147] Rule 5(9), IT Rules.
[148] Rule 5(9), IT Rules.

noted that currently the organization collecting and storing personal data is under no obligation to notify a data subject in the case of breach or change in privacy policy.[149] Another drawback of the rules is that while the information providers have the right to withdraw consent given earlier,[150] there are no guidelines laid down to indicate the course to be followed by the organization (that collects personal information), once the consent has been withdrawn.

e) Security Measures

The practices that aim to protect information from unauthorized access, disclosures etc., are designated as 'reasonable security practices' under section 43A of the IT Act.[151] The practices are supposed to be prescribed by agreement or law and in absence of the same they need to be prescribed by the central government. The security policies that are required to be put in place should cover technical, organizational and physical security measures. They are also required to follow some prescribed international security standards.[152] Such compliance will again ensure that the data protection regime that organizations are envisaging can match up to the international standards.

[149]Report of Group of Experts, *supra* note 116.
[150]Rule 3(7), IT Rules.
[151]Explanation (ii), § 43A, IT Act.
[152]The International Standard IS/ISO/IEC 27001 on "*Information Technology – Security Techniques - Information Security Management System – Requirements*" is specified to be one such security standard, Srinivasan, *supra* note 48.

VI. CONCLUDING REMARKS: PITCHING TOWARDS A CONSOLIDATED DATA PROTECTION REGIME IN INDIA

"India has a unique opportunity to draft a very modern data protection and privacy Bill which can be superior to what is happening elsewhere in the world."

- Nandan Nilekani[153]

In 2012 the AP Shah Report suggested the setting up of a consolidated legal data protection regime in India on the lines of the practices followed across the world.[154] Transparency, consent and accountability were identified as the fundamental building blocks of the regime.[155] These suggestions, however, were never implemented in the form of a law. A bill was introduced as a private members bill in parliament in 2009 by Baijayant "Jay" Panda titled "The Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill". It had the basic aim of protecting customers from unwarranted telephone calls from business promoters.[156] Other than the above, several other private members bills were also introduced on the subject that could never transform into a law.[157]

[153]Kunal Talgeri, *India Needs a Security and Privacy Law: Nandan Nilekani, Former Chairman*, UIDAI, ECONOMIC TIMES (Apr 29, 2017, 10:31 a.m.), http://economictimes.indiatimes.com/opinion/interviews/india-needs-a-security-and-privacy-law-nandan-nilekani-chairman-former-uidai/articleshow/58424580.cms.

[154]SupratimChakravorty, Soumyadri Chattopadhyay, *Imagining India's New Data Privacy Law*, BUSINESS LINE (Aug 17, 2017), https://www.khaitanco.com/PublicationsDocs/HinduBusinessLine-KCOCoverage17Aug17Supra.pdf.

[155]*Id.*

[156]Kazim Rizvi, *High Time India has a Right to Privacy Law*, LIVEMINT (Jul 30, 2017, 7:14 p.m.), http://www.livemint.com/Opinion/EcRER0qfjd1ooT1twFzdVJ/High-time-India-had-a-right-to-privacy-law.html.

[157]Rajeev Chandrashekhar, Vivek Gupta and Om Prakash Yadav in the years 2010, 2016 and 2016 introduced private members bill on the citizens right to privacy, *Id.*

Recently, the Unique Identification Authority of India informed a nine- judge bench of the Supreme Court that the centre had constituted a committee led by former Supreme Court judge B.N. Srikrishna to demarcate "key data protection issues" and on the basis of the same, suggest a draft data protection bill.[158] The committee was constituted on 31st July 2017. The ministry of Electronics and Information Technology will aid the panel to chalk out a data protection regime that is tailored per the Indian needs. The aim of the government is to come up with a bill that is similar to the "technology neutral" draft Privacy Bill prepared by the erstwhile Justice A.P. Shah Committee and submitted to the Planning Commission. At that point of time, no positive actions were taken in regard to the A.P. Shah committee.[159] It is to be noted that M.P. Baijayant "Jay" Panda again tabled a private members Data (Privacy and Protection) Bill, 2017 in the Lok Sabha under which he proposed that right to privacy be given the status of a fundamental right.[160] The bill also aims to differentiate between data collector and processor. The A.P. Shah committee draft bill further states that in the case of a data breach, it would be the responsibility of the intermediaries to inform the individual within a definite period of time.[161]

In the *Puttuswamy* judgement, the Supreme Court made overt recommendation to the centre to come up with a "data protection regime".[162] Accordingly, the Government of India set up a committee of experts under former Supreme Court judge B.N Srikrishna to make

[158]Krishna Rajagopal, *Privacy Argument Will Hit Governance*, The Hindu (Aug 2, 2017, 12:43 a.m.), http://www.thehindu.com/news/national/centre-constitutes-new-panel-under-former-sc-judge-to-prepare-draft-data-protection-law/article19402660.ece.
[159]*Id.*
[160]*Id.*
[161] Kazim, *supra* note 138.
[162]Puttuswamy, *supra* note 18 (holding that the "regime" would require a careful balance between the privacy interest of the individual and the larger concerns of the state).

policy suggestions on data protection and draft a bill on the same. Accordingly, the committee published the white paper on 27 November, 2017 in which it has made exhaustive recommendations, the scope and ambit of which, will be discussed in the present section.

A. An Analysis Of The Draft Bill Suggested By Srikrishna Committee

Before going into the contents of the white paper, some insight into the discussions of the committee members while working on the white paper, will be most resourceful. In response to an RTI filed by Mr. Paras Nath Singh, the committee revealed the minutes of its meeting dated 8thSeptmber, 2017 and 3rd October, 2017.[163]

The minutes reveal that Justice B.N. Krishna increasingly emphasised on the data protection regime being in the form of an umbrella law that will deal with varied facets.[164] The kind of regulatory framework that the committee envisages for India can be culled out from the four working groups that the committee has formed, namely-[165]

1. Working group on Big Data Ecosystem and other emerging technologies – which will deal with the technical aspects of the regime and analyse the pros and cons of data collection, and processing.
2. Working group on Scope and Exemption of Law- which will deal with issues of applicability of data protection laws. Applicability includes territorial limits, exemption from application etc.

[163]Apoorva Mandhani, *Justice B.N. Srikrishna Committee Discloses Minutes Of Meetings; Reveals Circulation Of Draft Data Protection Bill By MeiTY*, LIVE LAW (Feb. 12, 2018), http://www.livelaw.in/justice-b-n-srikrishna-committee-discloses-minutes-meetings-reveals-circulation-draft-data-protection-bill-meity/.
[164]*Id.*
[165]*Id.*

3. Working group on grounds of processing and rights and obligations of parties- which will deal with the core legal issues associated with the control and transfer of personal data collected.

4. Working group on enforcement- which will deal with timely and flawless enforcement of the laws.

From the above listing of the working groups it is clear that the committee is pitching for a structured and responsive regime that can embrace the enormity of the subject that it seeks to control, i.e., data. A perusal into the white paper would reveal that the committee is keen to adopt and implement international standards with adequate tweaks to keep it in sync with Indian best practises.[166]

As per the committee, an ideal data protection regime should be based on seven principles- namely, flexibility of law, applicability of law to both public and private sector, consent must be meaningful, informed and genuine, there should be minimal data processing, strict accountability of those responsible for data processing, creation of a data protection statutory authority and lastly, imposition of adequate penalties for any violation.[167]

To analyse the provisions of the committee better, it is imperative to do so in context of the three questions that form the premise of this study.

A. Protection of What-

[166]Committee Of Experts (Headed By Justice B.N. Srikrishna), White Paper On A Data Protection Framework For India (2017) (hereinafter Srikrishna Report).

[167]Vatsav Khullar, *Report Summary-White Paper on Data Protection Framework for India*, PRS Legislative Research, (Dec 1, 2017), http://www.prsindia.org/administrator/uploads/general/1514525011~~Report%20Summary%20-%20Data%20Protection%20Expert%20Committee%20White%20Paper.pdf.

The Report recognises that the aim of a data protection regime should be to uphold the autonomy of the individual. This autonomy can be protected by guarding the personal data related to the individual. Hence, the personal data should be such that a particular individual is the cynosure of the data. In other words, the data should be about the individual.[168] However, all information related to an individual would not come within the ambit of personal data, i.e., only the data that can potentially lead to the 'identity' of an individual would qualify.[169] Further, the report categorises health information, genetic information, information related to religious beliefs and affiliations, sexual orientation and information related to racial and ethnic origin as sensitive personal data that ought to be accorded a higher pedestal of secrecy and protection.[170]

B. Protection from Whom-

The report, in very clear terms, states that a huge chunk of personal data is being processed in both the public as well as private sector.[171] Noting that in jurisdictions like EU, the data protection laws apply to both the public as well as privates sector, the report calls for a similar regulatory framework for India as well.[172] Hence, as the report points out, the need is to come up with a data protection law that encompasses both the public as well as private sector. Almost in the same breath, the report also treads a cautious path by suggesting that certain

[168] *See supra* note 179, at 46.
[169] The report states as an example that though a car registration number would not directly reveal the identity of an individual it can possibly reveal the identity of the same individual when clubbed with other relevant information. Hence, the registration no. should qualify as personal data, *see Id*.
[170] *Id.* at 61.
[171] *Id*. at 12.
[172] *Id.* at 41.

public entities can be reasonably exempted from the rigours of the law.[173]

C. Protection to whom-

The report at every point seeks to grant protection to the individual. Noting that by 2020, global volume of digitally created data will reach 44 zettabytes, of which a large chunk will be data related to individuals, the report seeks to protect individuals' interest and uphold their right to privacy as recognised in the *Puttuswamy* judgement.[174]

B. The Road Ahead- Recommendations for a draft Data Protection Bill

The Srikrishna committee has adopted a consultative process to fathom the Indian opinion on the ideal data protection regime. Making recommendations on a proposed legislation of such length and breadth would require an effective balance of the interests of all the stakeholders involved. Here, the author attempts to address some key concerns that data protection regime in India ought to follow.

The proposed recommendations can be best understood under the following two headers-

a) <u>The Content of the Regime</u>

[173]Noting however, that it is highly doubtful if total exemption should be provide to any government entity from data protection laws. Also, borrowing from the Puttuswamy judgment, the report points out that for the well-defined categories of the departments of government and similar entities in the private sector, reasonable exemptions may be made.

[174]*Id*. at 11.

An ideal data protection regime in India should have immense clarity. Most of the legislations in India till date have only evasively discussed the definition and ambit of the key terms associated with data protection.[175]

The new data protection regime should include clear definitions of personal and sensitive personal information wherein the scope of the former should be wide enough to embrace all data through which an individual can be identified or is identifiable.

Further, given the millennial fears of the government slowly metamorphosing into a surveillance state, the law should accord protection not just against the private sector but also the government and other public bodies.

Also, both the data processor (the one who uses the data for a purpose) and the data controller (one who has general supervision over the data but doesn't necessarily use/process it) should be brought within the ambit of the law.

Emphasis should also be paid on the following aspects-[176]

1. The discourse on consent-

The consent should be explicit and unambiguous. For example, suppose a woman X works for a company. The company has all the details of the women including her mail-id. There are certain specific uses that her email can be put to about which X has notice. However, if the company were to enter into a contract with another company for

[175]As noted earlier, the IT Act 2008 as well as the IT Rules, 2011 accord protection only against "body corporate" and "persons who handle personal information under terms of a contract". None of them deal with the responsibility of the government for an alleged personal data breach. Further, the ambit of sensitive personal information under IT Rules, 2011 does not include information pertaining to race, religion, ethnicity etc.

[176]Parag Mathur, *What The Upcoming Data Protection Law Means*, LIVEMINT (Jan. 17, 2018), http://www.livemint.com/Money/qYWLeoRFYj8gjS2v3LEIzK/What-the-upcoming-data-protection-law-means.html.

sharing employee information that the latter plans to use for an employee survey, an explicit consent of X should be taken.

Further, the degree of consent should vary according to the type of personal information that is sought to be collected.

2. The amount and extent of data that should be sought-

The data controller should seek only that much data that is adequate for the purpose for which it is sought. This is the test of 'minimum necessary data required for a particular purpose'.

3. Techniques of enforcement-

The minimum standards that are expected out of a data controller/processor should be implemented in the form of 'best practises certifications'. Under this policy certificates of healthy data protection practises should be provided to public and private entities that deal with personal data.

4. Scope to erase personal data once shared-

An individual should have the right to, subject to some restrictions, exercise discretion with regard to the time period for which his/her personal data is available with the data subject. A right to be forgotten from the digital space is essential in a democratic country.

b) <u>The Structure of the Regime-</u>

1. Whether a single law should govern both the public and the private sector-

The *Puttuswamy* judgement recognised right to privacy as a fundamental right 'enforceable against the state'.[177] This judicial discourse however, leaves a pertinent question unanswered- what about the horizontal application of the right to privacy with respect to the private bodies? There is no clarity at present whether right to privacy can be enforced against private citizens

[177]Puttuswamy, *supra* note 18.

or not.[178] However, there can be no ambiguity in the assertion that when the enforcement mechanisms against the private and government bodies are different, there is no need for the same regulation to govern both of them.

Also, given the potentially coercive power of the state to extract information from the citizens (as contrasted form the more voluntarily nature of disclosure in the case of private bodies), a more robust regulatory mechanism should be devised to tame governmental manoeuvres in collecting personal data of citizens.

2. The Powers of the Data Protection Authority-

A perusal into the Srikrishna committee shows that it envisages a powerful authority that wields wide and punitive powers. The authority will presumably act in close cohesion with the government. If the authority gets the power to sieve through the data of private firms under the pretext of data audits, firms might spiral down into the realms of redtapism.[179]

It also needs to be noted that unlike jurisdictions like EU, India has often seen wide powers vesting in the hands of few (across the public or private sector). Clearly, under such circumstances, a centralised authority for data protection can have serious consequences for freedom of expression as well as freedom of economic competition. Hence, separate Data Protection Authorities should be made to regulate the public and the private sector.

[178]Prashant Reddy, *One Data Protection Law and Regulator to Rule Them All?*, THE WIRE (Dec, 2017), https://thewire.in/202497/data-protection-law-regulator-india/.

[179]The author takes the example of social networking sights to point out that all pervasive control of a regulatory authority over these social networking sites, might trample the ease with which views and opinions are shared on them. Under the guise of protecting the personal data of the individuals, the authority might assume control over the discretion of the individual regarding the type of information he/she wants to share. *Id.*

It is expected that in light of the positive developments in the international arena towards a comprehensive and uniform data protection regime, India will take effective steps towards materializing a comprehensive legal data protection framework. In developing a consolidated law on data protection, it is imperative that the government ensures the active involvement of all the stake holders, especially the data subject. Such a wholesome framework will channelize the big data revolution towards increased prosperity of the nation and its individuals.

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

*Navya Alam and Pujita Makani**

Abstract

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

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

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

I. INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

[5]*Id.*

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

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

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

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

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

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

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

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

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

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

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

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

C. Contextualization of the Bill

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

For instance, the European Union has methodically created a robust framework of law that is "economically dominant, locally secure, and morally defensible."10 The cornerstone of the EU data framework is protecting individuals' data while simultaneously bolstering the economy's growth. To achieve this, the EU and the European data industry have entered into a public-private partnership worth $2.5 million that "aims to strengthen the data sector and put Europe at the forefront of the global data race."11 Further, the EU has decided to overrule the existing e-privacy directive. The existing directive was limited to traditional forms of communication. The EU now wants to include "Over-The-Top" services such as Whatsapp and Facebook12 within its directive. This means that the user must grant explicit consent for internet companies to record and store communications for advertising purposes.

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

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

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

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

D. Language and Structure of the Bill

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

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

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

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

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

E. Lack of adequate safeguards

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

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

[14] *Id.* §23(2)
[15] *Id.* Statement of Objects and Reasons.

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

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

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

[16] *Id.* §26.

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

recoverable.

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

IV. CONCLUSION

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