SANCTITY OF PERSONAL DATA: A COMPARATIVE STUDY OF DATA PRIVACY LAWS IN EU, US AND INDIA

Written by ***Anisha Agarwal***

Executive Legal, HCL Infosystems

ABSTRACT

With increasing digitization of every sphere of the world, it is imperative to keep data secure. In this study, I intend to do an in-depth analysis of the existing Data Protection Laws in three countries, namely The United States of America, United Kingdom, and India. The paper will be a comparative study of data protection laws in the chosen jurisdictions to bring out their stance against GDPR. The paper discusses the pre and post GDPR scenario of EU followed by the existing legislation of US, in order to compare the approach of the two states. In the last segment, the fragments of Indian legislation to protect data are discussed with a focus on its obligation to become of GDPR complaint nation, if need be. The focus has been laid on Indian laws as the Indian judiciary took massive steps such the decision in the Puttuswamy case[i] granting the Indians citizen, right to privacy as a fundamental right and the recent B.R. Krishnan report on the Data privacy bill, shows the high intention for the same. The purpose of this comparative study is to point out the similarities between the chosen states with an emphasis on India and the paper aims to bring up the point of differences between the countries and serve as a basis of amendments that could be brought in the existing Indian data protection laws.

DATA PROTECTION LAWS: QUILLS V. BLANKETS, A BRIEF OF NEED FOR DATA PROTECTION LAWS IN US, UK AND INDIA

'"I see an animal less strong than some, less agile than others, but, on the whole, the most advantageously constituted of all'"[ii] Internet, an arrangement of millions networks, is the fastest mounting network in history.[iii] In the last three decades, its population has grown a million times over. The reason of its growth can be attributed to the 2 main purposes that it tends to accomplish, to assist as a "communication medium making end-to-end communication"[iv] possible and the generic task as an information database.[v]Tom Gaiety stated that "right to privacy is bound to include body's inviolability and integrity and intimacy of personal identity including marital privacy".[vi] Edward Shils explained privacy as "zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose".[vii] Warren and Brandeis have very eloquently explained that "once a civilization has made distinction between the "outer" and "inner" man, between the life of the soul and the life the body…the idea of a private sphere is in which man may become and remain himself".[viii]

The focus of governments throughout the globe, has shifted from regulation of cyber-space to protection of citizen's rights. Though most developing states are still at infancy stage regarding the framing of legislation much like India, but many developed jurisdictions such as of UK and US have already set a benchmark in this realm.

John Perry Barlow asserted, "[G]overnments of the Industrial World you weary giants of flesh and steel, I come from Cyberspace…[Y]ou have no sovereignty where we gather…[W]e have no elected government, nor are we likely to get one"[ix]. This opinion assumes a rent anarchism in the architecture of internet, which is per se outside the purview of institutional control. This conclusion has been opposed by Prof. Lawrence Lessig stating "code is law". The code, or rather the hardware along with the software that molds the cyberspace as it is today, in itself portrays a set of restrictions on how subjects shall behave. It has been succinctly quoted that "[w]e are all regulated by software now. It has become possible to imagine that the most basic aspects of democracy, society, and even life itself might be regulated by software. The US

federal government has tried to regulate privacy, advertising, and pornography by software". Hence, laying the foundation for structuring regulations to monitor online behavior.

Lately the scholars have debated "whether lextechnologica, has a sui generis character that requires a new set of legal rules". The first school of thought, promoted by jurists like David Johnson and David Post, states that "cyberspace has its own inherent jurisdiction and is capable of self-regulation." Whereas the second school of thought, professed by jurists like Professor Jack Goldsmith, propounds that "cyberspace doesn't have a sui generis character and current technological and legal tools, are sufficient to resolve claims, as those that arise in physical environment." The later school of thought of inherent regulation appears to be more apt in this century.

With increasing digitization of every sphere of the world, it is imperative to keep data secure. In this study, I intend to do an in-depth analysis of the Data Protection Laws in three countries, namely the USA, UK, and India. The idea behind choosing, U.K. is, it has one of the most robust law system in the world and given the enforcement of GDPR it has brought a revolutionary change whose tremors can be felt globally. Also, EU has been ahead for its time by incorporating privacy as their subject's fundamental right, which for most jurisdictions is a farfetched idea. The rationale behind choosing USA as the second country is that United States has one of the most advance IT Service Industry and spectacular start-up landscape. It resides more than a quarter of 3.8 trillion dollars global IT market which accounts for 1.14 trillion dollars US value adds GDP and 10.5 million jobs. Furthermore by 2015, US were hosting 100,000 Software and IT companies, making it hub for all data. Apart from being an IT hub, the US Supreme Court in *Griswold v. Conniticut*[x] granted right to privacy to its citizen. Additionally, in 1998, the US department of commerce established the safe harbor agreements to assist the US IT companies in complying with the EU regulations, therefore strengthening the relation between them and European business. The last country was chosen for two reasons, the personal reason being the author's ethnic roots. Further, the Indian judiciary and legislators have been constantly working towards better data privacy laws. The massive steps such the decision in the Puttuswamy case[xi] granting the Indians citizen, right to privacy as a fundamental right[xii] and the recent B.R. Krishnan report on the Data privacy bill, shows the high intention for the same. The economic reason being that if the economic surveys are to be believed that the service sector contributed 66.1% to GDP. Out of the said percentage IT sector "is expected to touch an estimated share of 9.5% of GDP and more than 45 percent in total services exports

in 2015-2016 as per NASSCOM".[xiii] The export in IT sector in itself raises 108 billion US Dollars which is much higher than the domestic sector contribution of 22 billion US Dollars. "Major markets for IT software and services exports are the U.S. and the U.K. and Europe, accounting for about 90 percent of total IT/ITeS exports".[xiv] NASSCOM Survey of 2014 reveals that "The UK and Continental Europe respectively accounted for 17.4% and 11.6% of India's IT/ITES services export"[xv]. The purpose of this comparative study is to point out the similarities between the chosen states with an emphasis on India and the paper aims to bring up the point of differences between the countries and serve as a basis of amendments that could be brought in the existing Indian data protection laws.

The paper is divided into 3 broad segments, starting with the EU data protection provisions, followed by an examination of the relevant US rules. With GDPR being the game changer, the effect of the same on the US, succeeded by the existing framework of the Indian Data Privacy Laws, is assessed and the nature of the dissertation would be a comparative study keeping GDPR as the basis for the same and suggest the need of amendments in the Indian approach, if any.

THE GLOBALIZATION OF PRIVACY: IMPLICATION OF RECENT CHANGES IN THE DATA PROTECTION LAWS OWNING TO GDPR

Pre- GDPR Scenario: EU Primary Law, EU Secondary Law and Council of Europe on Data Privacy Laws

To understand the data protection laws in the UK, one needs to look into the three components of EU law, i.e. the EU Primary Law which encompasses the Article 16 of TFEU, European Charter of Fundamental Rights and, Secondary Law which shall cover the rules and regulation to regulate the processing and transfer of data along with the restriction on the same, and lastly the Council of Europe which shall consist of Article 8 and 13 of ECHR and convention No, 108 and recommendation number R(87)15.

EU Primary Law

The implementation of the Lisbon Treaty in 2009 established the ground level of data protection law. The TFEU, in its 16th article, states that an individual has a right to protect its[xvi] data and paves the rules to protect the same.[xvii] Simultaneously, the Fundamental Rights of the

European Union which came into force under its article 7 and 8, ensures data protection and privacy for all.[xviii]

The Court of Justice of the EU preserves the right to apply and interpret the above-mentioned rights. These rights could be exercised by the court only after the abolition of the former pillar structures were put to rest by the Lisbon Treaty. The reason for the limited number of cases in this field could be attributed to the formerly restricted competence of the court. Though the courts have in recent years started taking suo moto initiative by becoming aware of their judicial powers, which is reflected in the increasing number of cases. The court passed a landmark judgment 2006/24/EC/(DRD)[xix] in April 2014, regarding the retrospective annulment of the Data Retention Directive which changed the scenario of the privacy laws. The decision had a remarkable effect on the power balance between the right of the individual over their data and the European Union and its member's right over the same. This case also paved way for significant rules for the interpretation of the Article 7 & 8 of CFR. The rules of interpretation of for the above mentioned article can be found in Article 52 CFR, as it lays down rules for the possible limitation of rights, because it codifies the landmark rulings of the court and has the similar approach, which was in addition to national constitutions, the fundamental source of inspiration for the EU fundamental rights. Article 52(1) establishes a procedural policy by stating that the limitations to the charter can be implemented by enforcing a law only, while ensuring that the right don't take away the essence of regulation and the restriction shall also justify the rule of proportionality, implying that the restriction is imposed for the greater good of public at large and are quintessential to safeguard the right and freedom of subjects. Every restriction has to go through a three step test to ensure the reasonability of the restriction: "firstly, it answers the question as to whether the essence of the rights are respected, secondly, whether the measure at stake meets the objective of general interest and lastly, whether the boundaries of proportionality, specifically appropriateness and necessity are met"[xx] The court on more than one instance recognized the restrictions "the fight against serious crime in order to ensure public security, the fight against international terrorism in order to maintain international peace as well as the prevention of illegal entry into the EU as objectives of general interest"[xxi]

EU Secondary Law

Even after 6 years of implementing the Lisbon treaty, the current legal structure for data protection is still similar to the former pillar format which differentiated among the laws made

within the former first and former third pillar. The first pillar in EU offered real participation rights to the EU parliament which got condensed into mere consultation rights with the third pillar structure, which presently consists of Title V of the TFEU. Similarly, various data protection rights exist in the secondary law, each varying in their scope of application and the power to protect the individuals. There is various reason for non-enforcement of the major piece of EU data protection, Directive 95/46/EC, one of which is the pillar heritage, Although the principles inscribed in the directive are the basis of the data protection standards, therefore they still are used for reference.

Prior to the adoption of the Libson treaty, there was no legal framework for data protection rules. Article 95 EC Treaty[xxii] which states the general harmonization clause is the foundation stone of the EC secondary data protection law.[xxiii] Directive 95/46/EC was enacted to serve a dual purpose of unrestricted movement of personal data and individual data protection rights.[xxiv] Furthermore, the same article is the basis of the Directive 2002/58/EC on privacy and electronic communications and to complete the circle, Regulation 45/2001/EC provided data protection rules for the artificial persons. This instrument prima facie echoes the Directive 95/46/EC to lay the foundation of the framework.[xxv]

One of the common instruments under the third pillar framework is Framework Decision 2008/977/JHA, adopted in 2008[xxvi], which proposes to lay an all-embracing data processing rules for EU.[xxvii] This instrument eliminates the specific rules for EU bodies, databases, domestic data processing, thereby limiting its applicability on data processing rules related to cross border activities of Member States.

The enforcement of the Lisbon treaty altered the EU's constitution like never before, by making Article 16 the basis for adopting an inclusive data protection legal structure. Although, the framework proposed in 2012, had strong glimpses of the former division into various policies. However the same has been replaced by the GDPR and DDPLE Sectoras these legislations portray a broad approach and are set to substitute the national data protection laws, and weave a smoother framework for the protection of data and individual rights in the same regards,. These instruments are applicable equally on the subject of member states irrespective of their status as an EU citizen. In absence of legitimate data protection instrument, before the enforcement of the GDPR along with ongoing negotiation process with regards to DDPLE, descending common EU principles for data protection is an arduous task,

Council of Europe

The Council of Europe played a significant role in the EU data protection framework through Article 8 of ECHR and the ECtHR case. Apart from that, Convention no. 108 and Recommendation R(87)15 also plays a role in the comprehensive convention's protection.[xxviii] Article 8 ECHR is the knight in shining armor for data protection. The relevance of Article 8 could not be underestimated, as prior to Lisbon treaty the CJEU didn't deliver any decision in data protection matters until 2009.[xxix] Before the enforcement to the treaty the court were refrained by the then established EU principles in this sector due to the constitutional division which was later done away with by the treaty. While the European Courts were restricted by the former EU and EC Treaties, the proficiency of the ECtHR permitted it to formulate central principles in this specific area.

The Article 8 along with Article 7 of CFR developed an all-embracing fundamental right in EU and Article 6 of TEU and para (3) makes it amply clear that the principle of EU law shall incorporate the fundamental rights of ECHR. Moreover,, the scope of convention's right[xxx] will be similar to the fundamental rights of EU corresponding to ECHR.[xxxi] The interpretation of Article 7 and 8 of the Charter, is thereby done keeping in mind the principles developed by the ECtHR while staying under the purview of Article 8, relating to data protection and privacy. Article 1 of ECHR dictates the scope of Article 8 ECHR, mandating the member states to ensure "everyone within their jurisdiction the rights and freedoms" stated in the ECHR, thereby implying that the rights guaranteed under the ECHR are available to every individual of the contractive state, inclusive of foreign nationals, given that they are subjects of one of the convention's states jurisdiction. Although Article 8 doesn't explicitly mention data protection, but the Strasbourg Court had repeatedly held that "the protection of personal data is of fundamental importance to a person's enjoyment of his or her respect for private and family life within the framework for this article"[xxxii]

Post GDPR Scenario: An Overview of GDPR

"The best way to get a bad law repealed is to enforce it strictly." The thought of Abraham Lincoln still stands true to this decade. More than 2 decades ago, the then EC felt the need to streamline the data protection measures among member states so as to assist EU internal and cross border data transfer. The problem resided in significant disparate levels of safeguards and

failed to offer legal assurance- neither for data subjects nor for data controllers and processors. The European community hence, adopted Directive 95/46/EC of the European Parliament and of the Council of 24th October, 1995[xxxiii]on the protection and free movement of personal data so as to homogenize the existing rights of individual with respect to data protection and transfer between EU member states.

Another fact to ponder upon is that the European Directives have to be adopted in the domestic laws in order to gain the enforceability. Thus, increasing the hassle for implementation in every member state. The data protection directive failed to deliver the desired effect within EU. The attempt to adopt the directive in the member state resulted in legal wrangle. The practices that were legal in one member state was illegal in another member state causing chaos among the controllers.[xxxiv]

In 2016, EU replaced the Data Protection Directive with GDPR. The GDPR so, adopted is the fruit of 4 years of negotiations and umpteenth amendments. The reason for distorted competition and stagnant economic activities in EU, was attributed to the mutilated data practices across EU which caused legal uncertainties among the member states. This issue of different legal regime was taken care by regulation by ease as it applied directly to the addressees without requiring any further process for implementation or enforceability. With constant safeguards throughout the EU, the prospective barrier for free movement of data have been eliminated to great extent.

The motive behind implementing GDPR is to regain the faith of the people across EU Internal market. In order to do so the enterprises will now have to comply with the new data protection obligations and also, come clean with respect to pre-existing mandates under GDPR. The framers considered the obstacles of a global economy and the trending technologies, business models and hence framed such regulation that would take into account various like factors to bring as many enterprises as possible under the ambit of GDPR.

Stepping into the legal aspect of the regulation, GDPR replaces the 28 different judicial and legal framework by a classic single legal framework.[xxxv] This would initiate a level playing field for all the enterprises (existing and potential) which in turn will have a positive impact on the business and the economy as a whole. To reduce the unnecessary and rather lengthy process of prior notification to DPA, GDPR stresses upon the principle of the accountability. It just doesn't end there, GDPR had introduced various provisions to account for transparency and

customer friendly policies, giving the term 'consent of consumer'[xxxvi] some meaning unlike earlier. GDPR has come up with weapons like the right to data portability, data protection by design and default, standard privacy icons to inculcate the seed for fair competition towards better data protection services and products. The deterrent approach has been incorporated to prohibit breach of notification and for assessing the impact of data protection.[xxxvii] On the similar lines, the data protection officers have been appointed to protect the fundamental right to data protection. The GDPR bestows 8 major rights on its subjects which are '"Right to be informed (Art.14), Right of access (Art.15), Right to rectification (Art.16), Right to erasure (Art.17), Right to restrict processing (Art.18), Right to data portability (Art.20), Right to object (Art.21) and Rights in relation to automated decision making and profiling (Art.22)."'

The concept of consent has finally been given the value it deserves. GDPR makes sure that the companies do not take advantage over the consumer using the legalese and illegible terms and conditions. The enterprises are now under an obligation to draft the form in plain language, also mention that consent can be withdrawn with the same ease with which it is given. Furthermore, through GDPR it has become obligatory on the member states to issue a breach notification within 72 hours of the data breach when it is likely to "result in a risk for the rights and freedom of individuals". Apart from the notification, the controllers shall also inform the consumer about the same "without undue delay". Another milestone achieved by GDPR is that it gives the consumer a right to question the controller, whether and for what purpose the personal data is being processed. To further increase the transparency, the controller is bound to provide an electronic copy of the data to the consumer, free of cost.[xxxviii]

GDPR also enhanced the Right to be forgotten. Also referred to as the "Data Erasure"[xxxix], the consumer retains the right to halt further processing of the data and ask the processor to erase his/her personal data at any given point. Article 17 outlines the condition for accessing the right, for example, the when the consent is withdrawn or when the data has ceased to be relevant for the purpose for which it was processed., while entertaining these requests the controller shall weigh the right of the consumer to the "the public interest in the availability of the data" and decide accordingly. In terms of data portability, the subject has the right to transmit the personal data that they have provided in a "commonly use and machine readable format" from one controller to another controller.[xl] Additionally, Privacy by design has been around for a while but it only after the enforcement of GDPR that it has become a mandatory requirement. Basically, it means that the protection of data shall be kept as a focus since the inception of

designing of the system rather than being an additional feature towards the later stage. Article 23 sets the platform for the same by explicitly stating that the controllers shall process the data which is sine-qua-non for the functioning of their system (data minimization).[xli]

Under the GDPR there is a drastic change with respect to the data processing activities. Earlier the controller had to notify about their activities to their allotted DPAs, which for MNC's was a nightmare considering the different notification requirements for member states. Now with GDPR, this mechanism has been replaced by the internal recordkeeping requirements and the DPO's will be appointed only for certain controllers.

Even the CJEU made it amply clear that there won't be any way of escaping the high level of protection for personal data in the EU after GDPR. The regulation would follow the line of principles set by the landmark cases like that of *Google v. Spain* ("right to be forgotten") and *Facebook v. Ireland* ("safe harbor"). The judiciary dealt with the problems of digital ecosphere by firmly deciding in the favor of market principle, and stern wording on international data transfers. The GDPR has raised the standard of data protection by making a clear statement as the single biggest digital market in the world. Enterprises all around the world are bound to comply with the GDPR standards, in order to gain access to the EU markets.

The afresh formation of the European Data Protection Board has provided them the authority to force the DPA's to have a similar interpretation and enforcement of GDPR. The DPA's are free to approach the Board's consistency mechanism in case they face any issues or inconsistency while interpreting the GDPR. In case the board fails to reach a consensus regarding the discrepancy, then the board has the liberty to take the final call, which would be binding on all the DPA's. However, if the individual or the DPA isn't satisfied with the decision of the board, they can approach the National Court or the CJEU respectively against the same. The motive behind this mechanism is to increase coherence among the national data protection laws. Though presently the task to adapt to the practical, unbiased and principle oriented regulation may seem monumental in nature it would reap the benefit in the same proportion in the coming years. If implemented effectively these regulations could be the ideal for every nation to amend theirs and live up to the ever-increasing pressure of globalization and digitalization.

CONTROL OVER PERSONAL DATA, PRIVACY AND ADMINISTRATIVE DISCRETION IN US: THE PARADOX OF AMERICAN DATA PROTECTION AUTHORITY

Legislations in US to Protect Personal Data: Fourth Amendment to the Constitution, Privacy Act, 1974, and Judicial Redress Act, 2015

Thomas L. Friedman believed that '"*[A]merica is the greatest engine of innovation that has ever existed, and it can't be duplicated anytime soon, because it is the product of a multitude of factors: extreme freedom of thought, an emphasis on independent thinking, a steady immigration of new minds, a risk-taking culture with no stigma attached to trying and failing, a non-corrupt bureaucracy, and financial markets and a venture capital system that are unrivalled at taking new ideas and turning them into global products."'*. US inhabits the most influential IT companies, from Google to Facebook, which makes the data protection laws of the country a game changer for the entire world. The legal framework of the US has various legal sources which govern the data protection rules of the US. In this study, I'll l consider the 3 major sources of the same. In order to carry a comparison between the US and EU, it is essential to summarily illustrate the brief of the sources and restriction of Data Protection Laws. As changes have been introduced by the USA Freedom Act recently, the same has been discussed in the last subpart of this section.

Fourth Amendment to the Constitution

The Constitution of the US doesn't have much to say when it comes to law enforcement in the context of data protection law. The fourth amendment to the constitution is the only recourse which gives slight protection against the intrusive law enforcement action, certain data such as of telephone or banking records are protected by the under "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[xlii]. However, the same applies only when the situation meets the criterion of "legitimate expectation of privacy"[xliii]. Though as the law goes, with every law, comes an exception, so, pertaining to this particular right, the exception stands that when a person voluntarily hands over his data to a third party, the same shall not the be entitled to protection and this is commonly referred to as the third party doctrine.[xliv] If we understand this correctly than one

shall notice that, a major chunk of personal data like the websites visited, the dialed phone numbers, the email addresses, and personal records like that of education and banking are outside the purview of the fourth amendment.[xlv] Further, the fourth amendment doesn't protect the foreign citizens.[xlvi]

Furthermore, the government in some cases justifies the application of the Fourth Amendment by stating "reasonable" government interests.[xlvii] In such cases, if the right still prevails the last resort with the government is to suppress evidence in the criminal proceeding and to award damages in the civil proceedings.[xlviii]

Despite the restriction on its application the judiciary recently relied on the fourth amendment to pass a landmark judgment which could loosely be interpreted to possibly establish a "right to deletion" of the ancient data held by the agencies. Also, despite having so much hysteria regarding privacy and data encroachment by the government, there is a gaping hole in the laws protecting the same. United States lacks a definite and concrete data protection legislation despite being one of the biggest IT hubs in the world/ globally. In fragments, the rights have been protected through various Acts, that the author shall be discussing in brief.

Privacy Act of 1974

The aim of the privacy act is to monitor the processing of data in the US. It regulates the usage, exposure and collection of personal data which is usually classified as "record" described as "including, but not limited to, his education, financial transactions, medical history, and criminal or employment history" containing "his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[xlix]It covers all types of federal agencies except the state/local or private agencies.[l]

The scope of Privacy Act covers the matter concerning to the record kept in a "system of records",i.e. database, which is defined as "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[li] This definition covers most of the databases except the ones which pertains to the mining activities.[lii] Further certain databases are preferred over the others such as those pertaining to the sensitive data regarding freedom of expression and association, physical and mental health records.[liii]

Unsurprisingly the protection of this act is also limited to US citizens or those with the intention to permanently establish there, excluding the foreigners from its purview until they reside permanently in the US.[liv]

Coming to the disclosure provisions '"no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."'[lv] Although there are 12 express limitations on the rule, most commonly used is that of "routine use" or for facilitating the government's process "for a civil or criminal law enforcement activity".[lvi] These exemptions largely negate the protection guaranteed under the rule to an individual. The rights of individuals are seriously inhibited by government protection to agencies which could be concluded from subtle instances like, the access to information is excluded to any information "Complied unreasonable anticipation of a civil action or proceeding", hence efficaciously restricting access rights. The other sort comings of the act were, that the legislation lacked provisions regarding data retention periods, absence of balancing of interest, exemption of the applicability of the rules in case of data maintained by the CIA and other law enforcement agencies, which was abused by FBI on regular basis.

Judicial Redress Act of 2015

The purpose of this legislation is to bridge the gap left by the Privacy Act of 1974. This act overcomes the shortcoming of the Privacy Act by giving the foreigners ("covered persons") of the so called "Covered Countries", the status similar to that of US citizens under the Privacy Act. In other words, the foreign nationals that come under the purview of this act will have access to the same remedies that US citizens have in case of data mishandling.

These protections are available to only the "covered records" which loosely includes the records maintained by the US agencies. All such terms are defined in the Privacy Act itself: '"transferred (A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and (B) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses."'[lvii] There

are many such instances which clearly indicate that the data transferred to non-designated sources will be outside the ambit of this act.[lviii]

Furthermore, a deeper analysis would give us an insight that the data which was transferred before the country became a "covered country" is excluded from the protection. Similarly, if the Attorney General has revoked the status of a designated country as a "covered country" then the individual belonging to that country loses its right to sue under this act.[lix] This again shows the United States narrow perspective when it comes to the protection of individual data processed by federal entities.

Another key observation would be that only 3 of the four remedies mentioned under the Privacy Act are available to the foreigners in this Act. The right to get damages, costs and attorney fees, under the 5 U.S.C. § 552a(g)(1)(C) if it is found that the agency is guilty if it "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record and consequently a determination is made which is adverse to the individual" is not covered at all. The major paradox of the act is that the data under its ambit is restricted to ""for purposes of preventing, investigating, detecting or prosecuting criminal offences", while affirmatively stating that the covered person shall be subjected to "the same limitations, including exemptions and exceptions" applicable on the individual under the Privacy Act,1964[lx],which in turn leads to the conclusion that given the encyclopedic exemptions stated in the Privacy Act, the already sectarian scope of application of rules would be further comprehensively diminished, if the same exemption are imposed.

Restrictions on Data Protection Guarantee by ECPA, FISA, PATRIOT and USA Freedom Act

It can be fairly concluded from the above discussion that the exemptions in the data protection legislation leave a broad scope for various discretionary interpretations. To add on to the list of exceptions, there are various other legislation in the US legal framework which further limits the rights of data protection. In this section, we shall, in brief, study some of such exceptions levied by the FISA, ECPA and the PATRIOT Act.[lxi]

Criminal Investigations under FREEDOM Act and ECPA

There are 3 main sources by which the personal information can be collected which are accessing the private databases and online resources, Administrative subpoenas and Court orders under ECPA.

The concept of data protection is bleak but not non-existent in an ordinary criminal investigation. One can't jump to general conclusion/ be presumptuous as there are some sector specific guarantees in certain legislation through the absence of general data protection structure for the private sector is still an issue to be contested by the senators of US. There are sector specific data control protection in the USA, as discussed there is no central legislation for the same and as a result private sectors are being overlooked. Thus, resulting in them escaping liabilities arising out of breach of data protection.

National Security Investigations in PATRIOT, FISA and FREEDOM ACT

Apart from the general criminal investigations, another major source of data collection is done via national inquiries provided in the PATRIOT Act and FISA.

The prominent provisions of FISA would be:

"Access to business records for foreign intelligence and international terrorism investigations","The metadata surveillance"An addition by FAA act which gives the US government the authority to collect data from any non-US person irrespective of his location The wide powers provided under the FISA are problematic not only for US non-citizens, they are also symptomatic of the disregard the United States has for data privacy in general.

Comparison between EU and US Approach Towards Data Protection

There is a blatant sense of ignorance if one believes that the EU and US could be compared with each other in the context of the data protection legislation owning to a fundamentally different approach towards the subject matter. However, certain striking similarities and differences could be stated for the academic purpose.

One of the glaring differences with respect to the comparison with the highest law the comparison with the highest law, the constitution of the EU itself provides for protection of personal data, though the same kinds of fundamental protection and privacy are not guaranteed

under the US constitution. EU started shaping its legislation to enable data protection right from the 1970's via landmark precedents from ECtHR cases and the incorporation of various data protection directive mentioned above. The US on the other hand was a late bloomer with the fourth amendment providing negligible protection.

The EU in this regard is rather well-prepared as it is armed with various strategies in favor of data protection. Some of the prominent features of the strategies are "rules on data quality standards, on sensitive data, independent supervision, the purpose limitation principle, rules on inter-agency exchange or transfer of data to third states, time limits for the retention of data, effective judicial review and access possibilities, independent oversight, proportionality elements, notification requirements after surveillance or data breaches, access, correction and deletion rights as well as rules on automated decisions, data security as well as technical protection".[lxii]Even though there are restrictions on the above stated rights as well but the same are subjected to the rule of proportionality and judicial review. Conversely, the US, on the other hand, has placed only limited focus to the above stated rights in their framework, like that of supervision or judicial review in ECPA.[lxiii] Moreover, the rights that still do exist in the US are overpowered by the unending list of the exceptions imposed in the façade of "national security interest" and are never weighed in proportional context.

US lacks in giving the same data protection to its subjects comparing to what EU has to offer as most of the guarantees offered by EU don't even exist in the US. Another divergence is that EU insists on restrictions on further usage and dissemination of data, whereas such principles can't be found in the US. The reason behind this is that their approaches are poles apart , while EU believes that transferring the data to the third party violates the fundamental rights and should be done in cases of utmost necessity with adequate justifications, on the other hand, a large amount of data transfers within the agencies seems to be the rule, rather than the exception. On contrary in EU, violation of an individual's fundamental right due to the existence of another legal legislation is an abundant ground for an individual to sue, as established above the same can't be said for the US. This could be inferred from the Klayman case, where the court stated that the plaintiff doesn't have the right to sue as they "lack[s] direct evidence that records involving their calls have actually been collected."[lxiv]

Another crucial distinction is regarding the subjects of the legislations. The EU provides the same data protection to all person irrespective of their nationality, or domicile, whereas US differentiates between US and Non-US person. This distinction is evident from the legislation such as FISA and the PATRIOT Act. Even the recent legislations like Judicial Redress Act or the FREEDOM Act fails to make any drastic or noteworthy changes in that perspective.

Fortunately, the present standard of data protection would not have any impact on the data sharing agreements of US-EU, for example, Safe Harbor Regime. Nonetheless, there is a pressing need for both the parties to increase their protection standards and bridge the gaps soon. The same was affirmed by the Advocate General Bot in the case of Schrems.[lxv]Yet, there are certain similarities which can't be ignored between these frameworks. One such instance is supervision, EU and US both have imbibed the concept of supervision and oversight, however there is a slight point of difference in their definition, where the former believe in supervision independent of the nature of the agencies whereas the latter is inclined towards the internal supervisory mechanism.

With regards to the above analysis, it could be safely concluded that even if we bring together all the US legislations and make them applicable to the EU citizens, it would still not hold a candle against the protection standard offered by the EU.

A BIRD'S EYE VIEW OF DATA PROTECTION LAWS IN INDIA

Existing Fragments of Data Protection in Indian Legislations

The Indian Constitution enunciates the right to freedom of speech and expression, which could be translated to freedom to express his/her opinion about certain things.[lxvi] Further, a person has the freedom of life and liberty, which can be taken only by the "procedure established by law".[lxvii] These articles can be inferred as the torch bearers of the right to privacy and data protection.

Personal information is whispered to be the personification of one's personality which is why the Indian courts have time and again reiterated that they believe that the right to privacy is a fundamental right. Judicial activism has interpreted the Article 19 and 21 to bring the right to

privacy under the ambit of fundamental rights. In *Govind v. State of M.P*[lxviii]., Justice Mathew delivered the majority judgment asserting that the right to privacy is a fundamental right and can be interfered with on the grounds of pressing public interest only. The concept of privacy has been played around with in various cases, interpreted differently in different situation. For some privacy was the "desire to be left alone" and for others, it meant the "desire to be paid for data and the ability to act freely".

Therefore, the right to privacy has been attributed to the deserved attention and cannot be fettered with unless for compelling reasons such as, in matters relating to national security and public interest. Currently, there is no special legislation which governs the subject matter of data protection or privacy. Although, there are various legislations which have certain safeguards for privacy and data protection. In this section, we'd read about some of the above-mentioned laws. The torch bearer for the IT Laws in India is IT Act,2000, which along with amendment of 2008 and associated rules covers the major chunk of data protection law. The IT Act provides remedies in case of a data breach from computer systems regardless of the location of the culprit, as long as the crime is committed on an Indian system. Additionally, this act has provisions against the unsanctioned use of a computer, computer systems, and data stored therein. Further, it creates personal liability for the same.[lxix] However, the internet or network service provider or the entities handling data are not expressly covered under this section. Consequently, all the enterprises which are entrusted with the duty of safe dissemination and processing of data such as vendors and outsourcing servicing providers are not under the ambit of this Act.

These liabilities are further weakened by section 79 of the IT Act, which pertains to 2 conditions of “knowledge” and “Best Efforts” while adjudicating the quantum of punishment.[lxx] In other words “a service or network provider could escape the liability under the provisions of this act if they successfully prove that the offense was commissioned without their knowledge, or that they had exercised due diligence to prevent the commission of the offense."[lxxi] However, it would be pertinent to note that in case an employee of accompany violates the provisions of the Act, then the key personnel (managers and directors) would be held personally responsible for the infringement of the IT Act.[lxxii]

The IT act primarily deals with the issues reading the legal recognition of the digital signatures and electronic documents, offenses and contravention, and adjudication mechanism for cybercrimes. The act was amended in 2008, which brought in the key features such that of focusing on data privacy and information security, defining terms like cybercafé, made digital signature technology neutral, defined the roles of intermediaries, inspectors, Indian computer emergency response team, introduced the crimes like child pornography and cyber terrorism in the act. We'd read about this act in detail towards the end of this section while comparing it with EU provision.

The Indian Penal Code can also be relied upon to claim relief in cybercrimes. The criminal law was drafted way back in 1860, so to except this legislation to be equipped with the provision regarding data protection would be futile. However, after the enforcement of IT act, the IPC was amended to include "electronic records" in its provisions relating to records, thereby placing them at par with the traditional documents.

Moreover, liability for the cybercrimes can be inferred from the related crimes.[lxxiii] For instance, section 463 deals with forgery and false documents, wherein if the accused attempts or forges the documents causing damage to any person, the same shall be punishable under section 465, which, if given a broader interpretation would cover the cases of email spoofing. Similarly, the case of identity theft could be covered under section 416 of IPC which related to cheating with impersonation and various cyber frauds can be covered under section 420. Courts in India have always focused on protecting individual rights. In that regard, broad interpretation of laws can be expected of them to make up for any legislative lacunae such as, when IT Act fails to establish what comes under the ambit of wrongful loss or wrongful gain[lxxiv] while pressing Section 43A[lxxvlxxvi] of the Act.

Similarly, the personal information collected under the CICRA Act are to be processed as per the privacy standards mentioned in the CICRA regulation. The entities which are responsible for the collection of the data are also responsible for any data leak or alteration. The Fair Credit Reporting Act and the Graham Leach Biley Act forms the basis of the stringent framework for the credit and finances of person. The Reserve Bank of India enunciates the principle which governs data privacy fundamental. With regards to globalization and increasing competition

among the market players, the software companies have taken upon them to take initiative towards data protection in order to gain the trust of the foreign investors. One of the said initiatives is The National Association of Service and Software Companies, which is the largest technology trade group which aims to improve privacy and data security. NASSCOM have come up with ideas like National Skills Registry, which is primarily a database of employees engaged in the IT services and BPO enterprises. The intention behind is to verify the credentials of a potential employee from within the industry. In addition to that, a self-regulated organization has been established whose purpose is to frame, monitor, and implement the privacy and data regulations for Indian BPOs. Private enterprises have also voluntarily imposed strict data protection rules to prevent the tampering of personal data by its employees as well. Impact of National Skills registry in light of data privacy

Comparison between GDPR and Indian Laws on Data Protection

As discussed earlier at the moment the enterprises all over the world are analyzing the influence of GDPR on their business. The reasons for the same have already been dwelled upon. The peculiar economic structural transition of India has not been hidden from anyone.

Giving regard to the gravity of the situation, India shall take every essential step to develop this sector of the economy, which presently depends on the adaptability and responsiveness of India towards the regulatory changes around the world. To retain the position of a dependable processing nation, India must examine and amend the legislation as per the global standards. This section will discuss the notable difference and similarity between the GDPR and IT Act and the notified rules.

To begin the comparisons let’s have a look at the objectives of both the legislation. GDPR has 3 objectives broadly which are “protection of natural persons when their data is processed, protection of their fundamental rights and freedoms with respect to data protection and freedom of movement of personal data for processing purpose. The Regulation confers protection to data subject as a matter of right". Additionally, GDPR reaffirms the rights granted by the Charter of Fundamental Right of European Union and Treaty on functioning of European Union.

Section 43A of the IT Act gives an insight about the objective of IT Act and rules which is to provide a model law to assist e-commerce in a smooth manner. Both regulations strive to promote a transfer of data for encouraging e-commerce. Though, GDPR is a step ahead as it not only intends to assist data transfer but also to protect the rights of the person throughout the processing of data. The principles of processing and collection of data is one head which grabbed the most attention during the framing of GDPR. The IT Act rules and GDPR both lay down the principle for data protection. The rule 5 of the IT act states that there should be lawful object behind collecting the information[lxxvii] and should be with regard to doings of an enterprise[lxxviii] for a time period required to fulfil the object to a collection in the first place.[lxxix] The data processing under GDPR is steered by "purpose, limitation, accuracy, storage limitation, integrity, confidentiality, and accountability."[lxxx] Both the laws have the same stand regarding the lawful objective behind the collection of data. Furthermore, The IT rules suggest that the data can't be retained for a longer period than required to achieve the object, the GDPR have some reservations on the same

The difference lies in the fact that the term "processing" has been defined under Article4(2) of the GDPR but the term 'processing' as a definite, concrete term has not been defined at all under the IT Act. Though a relation can be drawn by the usage of the word processing in definition of the term 'Data. An inference can therefore be drawn that since the word 'processing' has been used in defining "data". Furthermore, data has been included while defining information,[lxxxi] so, by applying the golden rule of interpretation, it could be said that the above-mentioned rules are also applicable to processing. However, GDPR takes another step by not only restricting the rules to a lawful purpose for data collection and retention but by supplementing them with rules pertaining to data integrity, transparency, fairness and safeguarding the data from illegal processing and damage, unlike IT Act.

Additionally, the fundamental of accountability is also a key feature of GDPR which makes the controller liable in case non-compliance with the principles of GDPR, the same can't be said for IT rules. The accountability of the controller is nowhere expressly mentioned in the legislation but a circuitous reading of Rule 5, could make up for the gap.[lxxxii] Oddly despite the lack of robust framework the IT rules has been quite comprehensive with the definitions by distinguishing between "sensitive data" and "information", both of them is governed by a

separate set of rules. For instance, the rule that there must be a lawful purpose to collect information regarding the activities of the corporation, applies to "sensitive personal data", the same is not applicable to "information". Similarly, the purpose restriction stated under rule5(5) applies to the "information collected", which doesn't include the "sensitive data" in its purview. The purpose behind this difference is still a mystery. GDPR, on the other hand, is concerned with the processing of "personal data" in general. Another point of difference is that IT rule 5 is not applicable to "company collecting personal data under a contractual obligation with another Indian or foreign company".[lxxxiii] This leads to an inference that the enterprises which directly get into a contractual obligation with natural persons to collect personal data are subjects of this principle, whereas the GDPR doesn't have any such stipulation.

The IT act since it was not created with the intent of protecting consumer information, doesn't have the same safeguards as GDPR. I believe that the courts through judicial interpretations can provide for regulation of data as well as processing.

Similarly, The lawfulness of processing is discussed in both the legislation, while the IT Rule 5(2)(a) states that in order to collect the sensitive data one needs to have a lawful purpose behind it as discussed earlier while the Article 5 makes it amply clear that the GDPR favours only lawful processing and Article 6 elaborates on the same. Both the legislation gives due regard to the consent of the data subject but GDPR wins this battle as well, as it describes the lawfulness at length. Further it has stipulations for processing that it shall pertain to one of the following stated matter only i.e. "performance of contract to which data subject is party, compliance with legal obligation to which controller is subject, protecting vital interests of data subject or another natural person, protecting public interest or in exercise of official authority vested in controller, fulfilling legitimate interests of controller or third party."

Additionally, the member states have the authority to specify further conditions. Also, if the controller needs to use the data for purpose other than that for which it was collected the same could be done, if the purpose of the latter is inconformity with the one for which the consent has actually pursued. The criteria for the same have been set out in GDPR. IT Act and Rules do not provide for lawful processing of data in the similar context.[lxxxiv]

The rights and liabilities for processing the personal data has been discussed in a generalized manner in GDPR. The personal data has been further categorized into "sensitive data"[lxxxv], which has per se the potential to infringe the fundamental rights and freedoms, if handled incorrectly.[lxxxvi] To abstain the tampering of such sensitive data it is classified as "special categories of personal data" and has to go through tougher procedures for being permitted to process.. Similarly the IT Act and Rules also provide special treatment to "sensitive personal data or information" under section 43A, the list of the same is given under Rule 3 of the IT Act. Biometric data, sexual orientation and health records are categorized as sensitive data by both GDPR and IT Act. Article 9 of GDPR covers "racial or ethnic information, political opinions, religious or philosophical beliefs and trade union membership,"[lxxxvii] as sensitive data which is excluded under the Rule 3 of the IT Act. On the other hand, GDPR excludes passwords and financial information, the same finds themselves with the IT Rules list.

Article 4(11) of GDPR defines consent at great length. Meaning and demonstration of the same is the fundamental pillar of the GDPR, with exceptional consideration to the consent of the child when information society is involved under Article 8. Under both the legislation the controllers are bound to seek the consent of the user before collecting the data[lxxxviii]. Additionally the user also retains the right to withdraw the consent at any given point. Though, the IT Act lags in defining the term consent and doesn't have any special provisions regarding the consent of a child. The consent could be vaguely inferred from rule 5 which makes it obligatory for the controller to obtain a written consent before collecting or using information or data. The rights granted by GDPR as discussed in the earlier section are not defined per se in the IT Act anywhere. Although, by applying the golden rule of interpretation, the existence of some the rights can be traced in the IT rules, though to expect them to be discussed in the detain which GDPR does would be a futile thought. One of the rights conferred in the IT Act is Right to Rectification can be loosely inferred from Rule 5(6) which confers the right on the data provider to "review the information" for amendment in case of incorrect or inadequate personal or sensible information. The same right is stated under Article 16 of GDPR with an additional stipulation that the controller is bound to inform the data provider before it discloses the same to a third party.

Right to be informed can also be read in between the lines of Rule 5(3) of the Act and Article 14 of the GDPR, both states that the data provider shall be informed about the purpose for the collection of data, the name and address of the agency and the recipients of the data, the

categories of the personal data. GDPR takes extra precaution by elaborating further conditions for the same. One of such instances is when a data is transferred to a third party additional safeguards have to be complied with to ensure fairness and transparency. Rule 5(7) of the IT Act and Article 7(3) of the GDPR have the right to withdraw their consent given earlier. The difference between the two is that the IT Act provides and "option" to withdraw the consent the GDPR provides the "right" to do the same.[lxxxix] Additionally the GDPR bounds the controller to erase the data under Article 17, once the consent is withdrawn by the data provider without the undue delay.[xc] The IT act fails to answer the question that what would happen to the data once the consent have been withdrawn except that the body corporate have the liberty to refuse the goods or services for which the information was seek.

The IT Act also has policies to secure the data through privacy policies and "reasonable security practices and procedure". The rules state that it is a mandate on every website to publish their privacy policy. The mentioned policy shall disclose the type and purpose of collection, disclosure regarding information and the security polices employed to secure the information. A lawful contract is a sine qua non for collecting personal information under the policy. Rule 8 determines the standard of security practices and the procedures. For an organization to pass the test of reasonable security practices and procedure, two stipulation shall be complied with, first is the implementation of security standards and program and the second is the implementation of comprehensive documented information security program and information security policies. If any organization fails to adhere to the same, they shall be liable under section 43A of the Act, whenever their illegal gain or loss due to inadequate attempts to protect the data. GDPR is one step ahead in this segment as well as, under GDPR, the organization are obliged to comply with data processing policy by design and default. The compliance can be portrayed by adopting methods like pseudonymisation, privacy impact assessment, appointment of data protection officers, maintenance of records of processing activities and notification of data breach.[xci]

The compensation granted under the Data Protection Law may be on a per day basis[xcii] on which the upper limit is fixed usually by the adjudication body[xciii], and that limit is at the depened on variable parameter[xciv]. With regards to compensation for damages due to infringement of data protection, IT act and GDPR have adequate provisions under section 43A and Article 82 respectively. However, both legislations have granted some exemption from liability. According to the 82(2) of GDPR, the controller can escape the liability if he

successfully proves that the infringement was beyond his control and he isn't responsible for the same. Similarly, if the controller satisfies the conditions of implementing adequate security measures to protect the information, he too shall not be liable to pay compensation under the IT Act. The distinction between the laws lies in the nuances i.e. under the IT Act, the competent authority varies with the amount of compensation. For instance, the Sec. 46(1A), the adjudicating officers have the jurisdiction to entertain the dispute up to 5 crores only, for the dispute whose valuation exceeds this amount will have to approach the competent court. On the contrary, GDPR has given the absolute power to the Member State's court to adjudicate the matter without any bar on the pecuniary jurisdiction, but it shall be done in accordance with the case laws as developed by the European Court of Justice. Another distinction lies in the fact that IT Act makes it difficult to make successful claims against privacy breach by mandating the requirement to establish that there had been an illegal loss or gain due to the breach, unlike the GDPR which doesn't require the aggrieved to prove mens rea, similarly information disclosure has grave repercussions under both the laws. 72A of IT Act imposes a fine up to 5 lakh INR whereas GDPR imposes a exemplary fine up to 10,000,000 EUR or 2% of total wide turnover of preceding financial year, whichever is higher. Though, the difference between the two is that IT Act imposes criminal liability under section 72A in case of breach of data confidentiality contract, unlike GDPR which doesn't impose criminal liability and rather resort to hefty administrative fines.

There exists two-fold redressal mechanism under GDPR, the aggrieved could either file a complaint with a supervisory authority or he can approach the judiciary to get justice. Under GDPR, the data subject doesn't need to exhaust all his administrative remedies before approaching judiciary. The IT Act puts the Adjudicating officer, designated by the enterprise, to redress the grievances related to processing of information. He has the power to investigate the matter and decide the quantum of compensation as well. An appeal against the adjudicating officer lies with the Cyber Appellate Tribunal[xcv]. Despite clarifying the pecuniary jurisdiction of the adjudicating officer, the competent court for matters above 5 crores has not been stated for the purpose of filing a complaint under section 43A of the Act. Further, the IT Act creates a criminal liability under section 72A for disclosure of lawful contract. It "falls short of creating a private right of action on behalf of individuals whose data is being handled by any third parties because it is still cast as a penal provision and does not create a private right of action in civil law…an individual cannot file a suit in civil court under this section as it does not create

a statutory right to damages or compensation, that is, there is no private right of action for damages in civil law". Though, the procedure to approach in absence of civil court, to impose criminal liability is ambiguous.

Similarly, both the laws have provisions for data transfer[xcvi]. Under GDPR the stipulation for data transfer are stated in the Chapter V, Article 44 to 50.[xcvii] The GDPR permits data transfers provided that the adequacy decisions[xcviii] or appropriate safeguards in absence of former are met. In absence of the above mentioned, additional conditions are also listed. Furthermore, the enforceability of the decisions passed by other courts and administrative authorities of other countries depends on the presence of the international agreement in force between the third country and the member states. The IT Act covers this aspect in Rule 7, which states that the data transfer is permitted only when the transfer is essential to fulfil the obligation under a lawful contract between the body corporate and data subject. The difference between the laws lies in the factors for adequacy of the safeguards, GDPR calls for additional safety measure apart from the one mentioned in IT Rule 7,which are "Rule of law, human rights, fundamental freedoms, relevant legislations, access of public authorities to personal data, data protection rules, rules for onward transfer of personal data to third country or international organization, case law, effective and enforceable data subject rights, effective administrative and judicial redress for data subject whose personal data is being transferred, existence and effective functioning of independent supervisory authorities for ensuring and enforcing compliance with data protection rules, international commitments undertaken ."[xcix] The various condition to match the appropriate safeguards include "Existence of legally binding and enforceable instrument between public bodies or authorities, existence of binding corporate rules, adoption of standard protection clauses adopted by commission, adoption of standard data protection clauses by supervisory authorities, approved code of conduct along with binding commitments, approved certification mechanism, binding corporate rules."[c]

BEYOND SAFE HARBOR: THE CHANGES THAT THE USER HAS BEEN UNCONSCIOUSLY LONGING FOR

On paper India has legislation like IT Act, 2000 and associated rules to account for data protection standards. Although, the benchmark set by GDPR is very high for the existing data protection laws scenario, India will have to work them out accordingly. There are various

significant Missing elements such as of breach notification, appointment of data protection officers and alike have to be incorporated in the Indian Law as well, that would further make the Data protection laws stringent. Moreover, the lack of deterrence through penalty in India is most likely to divert the business opportunities to safer locations which qualify as data secure states.

Given the stipulation of GDPR for data transfer, India shall instantaneously look for similar model contractual clause in an arrangement to qualify as a data secure location. Furthermore, EU Commission has commissioned two sets of contractual clauses.[ci] The first one pertains to the data transfer among the controllers and second pertains to data transfers to processor established outside EU\EEA. However, with reference to the Schrems case, the validity of the contractual clauses is under the scrutiny of the Irish Data Protection Commissioner[cii] Amidst the ongoing legal proceeding before the Irish High Court, the decision is waited. Irrespective of how attractive GDPR looks on paper, the act is no exception to the rule that no legislation is perfect, naturally there are imperfections like the chances of the data to escape from GDPR as the devil lies in the details, the wording while reiterating that the EU would have extra territorial affect states that "where the processing activities are related to the offering of goods or services" to that person. The expression "the offering of goods or services" is subject to disparate interpretations. Similarly, another route for non-EU data controller for escaping GDPR is that the data is only under the scrutiny of GDPR, when the "*the processing activities are related to the offering of goods or services* to the individual in the EU", otherwise the same could be processed for separate purpose without GDPR's monitoring the same. Another flaw lies in the right of data subject to have access to data, however given the data chain that forms under GDPR, the controller is not obliged to name the name of the controller but to just give the categories of recipients, so, how would a data subject know whom to ask question regarding the processing of their personal data and also the phrases "inferred data" and Legitimate interest" leaves a vast scope of interpretation.

While all the jurisdictions around the globe are succumbing to the pressure to comply with GDPR and raise their data privacy standard, blatantly adopting the same measure wouldn't benefit the state in long run. The attempt of Justice B.R. Krishna committee to draft the Indian Privacy Code,2018, is arching for the Indian domain, it is amusing and disheartening that the committee preferred to view the data privacy through the lens of innovation and a "free and fair digital economy".it is pertinent to note that the Indian judiciary while deciding the Puttiswamy

case unequivocally recognized that privacy was quintessential to the to human values of liberty, autonomy and dignity, the constitution of committee in the light of this judgment signaled towards seriousness of the government to regulate the through law the indiscriminate use of personal data, hence it could be established that there was no need to carve out a discreet fundamental right to privacy. Notwithstanding the government's view, it was obligatory on the committee to honour courts' words to empower the individual and interpret the constitutional rights articulated by it accordingly, rather keeping this as objective that the individual dictate the terms over the their data, the committee seemed to be fixated on stimulating the digital economy, and perceives the state as the key facilitator in this regime. The committee's comprehension of the mandate is evident in the very beginning of the report, from the title of the 1st chapter "A free and fair digital economy", which addresses India's approach grounded on the nation's developmental need, which could be loosely interpreted as, the need of restriction on privacy can be attributed to nation's interests of innovation and delivery of services, which is reminiscent of states' contention while adjudicating that the individual rights must pave way to welfare considerations, which was out rightly rejected by the judiciary stating that individual freedoms are essential prerequisites for people to enjoy social benefits. It can be best described as a fragmented landscape with grave associated risks, while EU's focus was to make data safe, India seeks also to emancipate the data subjects by granting them the power to access, manage and move data and further India's vision includes "account aggregators" who'd facilitate the transfer of data. This vision of India not only needs technical backing but also core and advanced technical aid, which most believe could be met by the aadhar "account aggregators architecture", however the same has been in limelight lately for multiple data breach. It could be fairly concluded that if the account aggregator fail to keep the data secure, not only the data subjects, but the enterprises transacting in data in India, will have to face the repercussions as the enterprise would be equally blamed for the breach, even if they hadn't been on fault, which would cost the significant goodwill loss, and in worse case face legal liability due to ambiguous legal regime. Another major risk is losing the title of critical innovation hub[ciii], innumerable emerging technologies rely on data flow, internet service being one of them, stringent data regimes like that of data localization[civcv]requirements, would be a hurdle for the enterprises involved in the same[cvi] as it would substantially increase the compliance costs, diverting their finances from innovation towards the former, would naturally discourage them for investing in this region.[cvii]

Instead of mirroring GDPR, the Indian data privacy bill shall aim to incorporate reasonable fundamentals like that of technology agnosticism, holistic application, informed consent, data minimization, controller accountability, structured enforcement and deterrent penalties as a staggering array of MNC and Indian start-ups are progressively transforming India, and taking into consideration the increasing adoption of technology and the internet, the gigantic customer base, and the governments persistent efforts through scheme such as of "digital India", data protection measures that could prejudice enterprises from entering or sustaining in Indian market can remarkably undermine the global ambition, while striping India of essential socio economic benefits of renovation. Given that the Indians have little choice in handing over the personal information while interacting with the government, the committee would have done well to give consideration to individual rights over ambiguous nations of renovation. Let's hope the state will revisit the gaps and pass a bill that actually bolsters the fundamental rights in this regard and bring India at par the international standards.

BIBLIOGRAPHY

Statutes

- Judicial Redress Act. of 2015
- Privacy Act of 1974
- USA PATRIOT Improvement and Reauthorization Act of 2005
- PATRIOT Act Additional Reauthorizing Amendments Act of 2006
- Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act Of 2001
- Electronic Communications Privacy Act of 1986
- Sunsets Extension Act of 2011
- Constitution of United States of America, 1787
- Foreign Intelligence Surveillance Act of 1978
- Constitution of India,1950
- Information Technology Act, 2000
- Information Technology Rules
- Indian Penal Code,1860
- Credit Information Companies (Regulation) Act, 2005
- Credit Information Companies Regulation, 2006
- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No. 108 (in the following: Convention No. 108)
- General Data Protection Regulation, Regulation (EU) 2016/679

Books

- Rowena Rogues &VagelisPapakonstantinou, *Privacy and data protection seals.*
- Paul Voigt & Axel von dem Bussche, *The EU general data protection regulation (GDPR)* (2017).
- Alice Keefer & Tomas Baiget, *How it all began: a brief history of the Internet*, 31 VINE 90-95 (2001).

- J. R Okin, *The Internet revolution* (2005).
- ArdiKolah, *The GDPR handbook* (2018).
- Alan Calder, *EU GDPR* (2016).
- Apar Gupta, *Commentary on Information Technology Act*, 269 (Lexis Nexis, 2013).
- Alan Westin, *Privacy and Freedom*, (Atheneum, 1967).

Cases

- Govind v. State of M.P., AIR 1975 SC 1378.
- Henke v. U.S. Department of Commerce, 83 F.3d 1453 (D.C. Cir. 1996).
- Klayman v. Obama, United States Court of Appeals, District of Columbia Circuit.
- Smith vs. Maryland, 442 U.S. 735 (1979)
- Katz vs. United States, 389 U.S. 347 (1967).
- ACLU vs. Clapper, No. 14-42 (2nd Cir. May 7, 2015).
- United States v. Miller, 425 U.S. 435 (1976).
- United States vs. Verdugo-Urquides, 494 U.S. 1092 (1990).
- Griswold v. Connecticut, 381 U.S. 479
- Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
- Case C-291/12, *Schwarz*
- CJEU, C-293/12, *Digital Rights Ireland*
- *Z. v Finland*, Application no. 22009/93
- *Peck v. United Kingdom*, Application no. 44647/98

Journals

- Daniel Solove, Privacy Self-management and the Consent Dilemma, 126 (2013) Harvard Law Review.
- Blanca Gordo, "Big Data" in the Information Age, (2017) 16 City & Community.
- UNION BUDGET & ECONOMIC SURVEY, Indiabudget.gov.in (2018), https://www.indiabudget.gov.in/budget2015-2016/survey.asp (last visited Jul 26, 2018).
- UNION BUDGET, Indiabudget.gov.in (2018), https://www.indiabudget.gov.in/ (last visited Jul 26, 2018).

- IT &ITeS Industry in India: Market Size, Opportunities, Growth...IBEF, Ibef.org (2018), https://www.ibef.org/industry/information-technology-india.aspx (last visited Jul 26, 2018).
- Peter Szczekalla, Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus (eds.), European Union Treaties. A Commentary. Treaty on European Union, Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union, (2015) 130 DeutschesVerwaltungsblatt
- Sreenidhi Srinivasan and Namrata Mukherjee, _Building an Effective Data Protection Regime ‘, Vidhi Centre For Legal Policy (2017).
- Fabio Balducci Romano, The Right to the Protection of Personal Data: A New Fundamental Right of the European Union, (2013) SSRN Electronic Journal.
- Tuomas Ojanen, Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 10 European Constitutional Law Review 528-541 (2014).
- T. Wisman, Introduction: Data Protection in All Directions, (2017) 399-401European Data Protection Law Review.
- L. Brouwer, Eurodac: Its Limitations and Temptations, (2017) 399-401 European Journal of Migration and Law.
- S. Peers, Finally 'Fit for Purpose'? The Treaty of Lisbon and the End of the Third Pillar Legal Order, (2008) 47-64 Yearbook of European Law.
- Ronald Leenes, Paul De Hert& Yves Poullet, European Data ProtectionIn Good Health? (2012).
- Jack Hyland, Data Protection in EU Businesses: An Introduction to GDPR, (2017) 146-148
- DBS Business Review
- Lukas Feiler, NikolausForgó& Michaela Weigl, The EU General Data Protection Regulation (GDPR).
- Melanie Dulong de Rosnay& Andres Guadamuz, *Memory Hole or Right to Delist?*, RESET (2016).

- Minjung Park, Sangmi Chai &Myoungjun Lee, A Study on the Establishment of Data Protection Officer (DPO) Position under GDPR Enactment, (2018) 427-438 The Journal of Korean Institute of Communications and Information Sciences.
- P. T. J. Wolters, The security of personal data under the GDPR: a harmonized duty or a shared responsibility? (2017) 165-178 International Data Privacy Law.
- Elizabeth Goitein&Faiza Patel, What went wrong with the FISA court (2015).
- Caspar Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights 474,405 (2013).
- Jack Hyland, Data Protection in EU Businesses: an Introduction to GDPR, (2017) 146-148 DBS Business Review.
- Andreas Wiebe& Nils Dietrich, Open Data Protection - Study on legal barriers to open data sharing - Data Protection and PSI (2017).
- Erne Mraznica, GDPR: A new challenge for personal data protection, 46 Bankarstvo (2017) 166-177
- EnginBozdag, Data Portability Under GDPR: Technical Challenges, SSRN Electronic Journal (2018).
- Marina ŠkrinjarVidović, Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities, 11 Croatian Yearbook of European Law and Policy (2015).
- Tom Gaiety, "Right to Privacy*"* Harvard Civil Rights Civil Liberties Law Review 233.
- Edward Shils, "Privacy: Its Constitution and Vicissitudes", Law & Contempt Problems (1966) 281.
- Samuel Warren & Louis D. Brandeis, "The Right to Privacy", (1980) 193 Harvard Law Review.
- Kamlesh Bajaj, Promoting Data Protection Standards through Contracts: The Case of the Data Security Council of India, (2012) 131-139 Review of Policy Research.
- A. Wankhede, Data Protection in India and the EU: (2016) 70-79 European Data Protection Law Review
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 5 (2011).
- Vidhi Agarwal, Privacy and data protection laws in India, (2012) 205 International Journal of Liability and Scientific Enquiry.

- Dr. Ajay Kumar Garg & Shikha Kuchhal, Data Protection Laws in India: A Comparative Study, 75-76 (2011) Indian Journal of Applied Research.
- Erne Mraznica, GDPR: A new challenge for personal data protection, (2017) 166-177 Bankarstvo.
- P. T. J. Wolters, The security of personal data under the GDPR: a harmonized duty or a shared responsibility? (2017)165-178 International Data Privacy Law.
- Sandeep Mittal I.P.S., Old Wine with a New Label: Rights of Data Subjects Under GDPR, (2017) SSRN Electronic Journal.
- Julian Wagner, The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? (2018) International Data Privacy Law.
- J. H. Saltzer, D. P. Reed & D. D. Clark, End-to-end arguments in system design, 2 ACM Transactions on Computer Systems 277-288 (1984).
- Lee Bygrave, _Data Protection Law: Approaching Its Rationale, Logic, and Limits‘ 2 , (2002)Kluwer Law International.
- Aimée Hope Morrison, An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace', (2009) 53-71 New Media & Society.
- Jerry Kang, Information Privacy in Cyberspace Transactions‘,(1998) 50 1193, 1202-03 Stanford Law Review
- Maria Tzanou, *Data protection as a fundamental right next to privacy? Reconstructing‘ a not so new right*,‘ (2013) 88 International Data Privacy Law.
- Erica Fraser, Data Localisation and the Balkanisation of the Internet ‘,(2016) 359 SCRIPTed.
- Srikrishna, B., et. al. (2018). *White paper of the committee of experts on a data protection framework for India*. [online] Available at: http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited [Accessed 4 Aug. 2018].

REFERENCES

[i]Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

[ii] Jean-Jacques Rousseau, *Discourse on the origin and Foundations of Ineuqlity among Men*, 11 in *Rousseau's Political Writings* (Alan Ritter & Julia Conaway Bondanella eds. 1988)_

[iii] Alice Keefer & Tomas Baiget, *How it all began: a brief history of the Internet*, 31 VINE 90-95 (2001).

[iv] J. H. Saltzer, D. P. Reed & D. D. Clark, *End-to-end arguments in system design*, 2 ACM Transactions on Computer Systems 277-288 (1984).
[v] J. R Okin, The Internet revolution (2005).
[vi] Tom Gaiety, "*Right to Privacy"* Harvard Civil Rights Civil Liberties Law Review 233.
[vii] Edward Shils, "*Privacy: Its Constitution and Vicissitudes*", Law & Contempt Problems 281 (1966).
[viii]Samuel Warren & Louis D. Brandeis, "*The Right to Privacy*", Harvard Law Review 193 (1980).
[ix]Aimée Hope Morrison, *An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace'*, 11 New Media & Society 53-71 (2009).
[x] Griswold v. Connecticut, 381 U.S. 479
[xi]Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
[xii] "right to privacy would encompass the right to informational privacy, which recognises that an individual should have control over the use and dissemination of information that is personal to her"
[xiii]UNION BUDGET & ECONOMIC SURVEY, Indiabudget.gov.in (2018), https://www.indiabudget.gov.in/budget2015-2016/survey.asp (last visited Jul 26, 2018).
[xiv]UNION BUDGET, Indiabudget.gov.in (2018), https://www.indiabudget.gov.in/ (last visited Jul 26, 2018).
[xv]IT &ITeS Industry in India: Market Size, Opportunities, Growth...IBEF, Ibef.org (2018), https://www.ibef.org/industry/information-technology-india.aspx (last visited Jul 26, 2018).
[xvi] American Civil Libertes Union v. Reno, 929 F. Supp. 824,830-31
[xvii]Peter Szczekalla, *Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus (eds.), European Union Treaties.A Commentary. Treaty on European Union, Treaty on the Functioning of the European Union, Charter of Fundamental Rights of the European Union*, 130 DeutschesVerwaltungsblatt (2015)
[xviii]Fabio Balducci Romano, *The Right to the Protection of Personal Data: A New Fundamental Right of the European Union*, SSRN Electronic Journal (2013).
[xix]TuomasOjanen, *Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*, 10 European Constitutional Law Review 528-541 (2014).
[xx] Compare: CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*
[xxi] Case C-291/12, *Schwarz*, Judgment of the Court of 17 October 2013 (in the following: CJEU, C-291/12 *Schwarz*), para 37.
[xxii]today Article 114 TFEU
[xxiii]L. Brouwer, *Eurodac: Its Limitations and Temptations*, 4 European Journal of Migration and Law 231-247 (2002).
[xxiv] Directive 95/46/EC "processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".
[xxv]T. Wisman, *Introduction: Data Protection in All Directions*, 3 European Data Protection Law Review 399-401 (2017).
[xxvi]S. Peers, *Finally 'Fit for Purpose'? The Treaty of Lisbon and the End of the Third Pillar Legal Order*, 27 Yearbook of European Law 47-64 (2008).
[xxvii] "Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed
in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60–71 (in the following: Framework Decision 2008/977/JHA)."
[xxviii] "Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal
Data, 28 January 1981, CETS No. 108 "
[xxix] "However, it repeatedly referred to the guarantees developed by the ECtHR with regard to Article 8 ECHR when
data protection issues in internal market matters were the subject of EU cases."
[xxx]Article 52 (3) CFR.
[xxxi] Ronald Leenes, Paul De Hert& Yves Poullet, European Data Protection In Good Health? (2012).
[xxxii] Compare: ECtHR for instance in *Z. v Finland*, Application no. 22009/93, Judgment of 25 February 1997, para
95; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para 78;
[xxxiii]Alan Calder, EU GDPR (2016).
[xxxiv]ArdiKolah, The GDPR handbook (2018).

[xxxv]Jack Hyland, *Data Protection in EU Businesses: An Introduction to GDPR*, 1 DBS Business Review 146-148 (2017).
[xxxvi]"In democratic societies, there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth…and in the need to maintain social processes that safeguard his sacred individuality" *See:* Alan Westin, Privacy and Freedom, (Atheneum, 1967).
[xxxvii]Lukas Feiler, NikolausForgó& Michaela Weigl, The EU General Data Protection Regulation (GDPR).
[xxxviii]Erne Mraznica, *GDPR: A new challenge for personal data protection*, 46 Bankarstvo 166-177 (2017).
[xxxix]Melanie Dulong de Rosnay& Andres Guadamuz, *Memory Hole or Right to Delist?*, RESET (2016).
[xl]Minjung Park, Sangmi Chai &Myoungjun Lee, *A Study on the Establishment of Data Protection Officer(DPO) Position under GDPR Enactment*, 43 The Journal of Korean Institute of Communications and Information Sciences 427-438 (2018).
[xli]P. T. J. Wolters, *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?* 7 International Data Privacy Law 165-178 (2017).
[xlii]Smith vs. Maryland, 442 U.S. 735 (1979)
[xliii]Katz vs. United States, 389 U.S. 347 (1967).
[xliv]ACLU vs. Clapper, No. 14-42 (2nd Cir. May 7, 2015).
[xlv]United States v. Miller, 425 U.S. 435 (1976).
[xlvi]United States vs. Verdugo-Urquides, 494 U.S. 1092 (1990).
[xlvii] Elizabeth Goitein&Faiza Patel, What went wrong with the FISA court (2015).
[xlviii]Caspar Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights 474,405 (2013).
[xlix] U.S.C., 552a(a)(4).
[l] U.S.C., 552a(a)(1).
[li] U.S.C., 552a(a)(5).
[lii]Henke v. U.S. Department of Commerce, 83 F.3d 1453 (D.C. Cir. 1996).
[liii] U.S.C., 552a(e)(7) and U.S.C., 552a(f)(3).
[liv] U.S.C., 552a(a)(2).
[lv] U.S.C., 552a(b).
[lvi] U.S.C., 552a(b)(3) and (7).
[lvii]Judicial Redress Act., 2(h)(4) (2015).
[lviii]Judicial Redress Act., 2(e), (f)
[lix]Judicial Redress Act., 2(a),(d),(h)
[lx]Sections 2(a) and (c) of the Judicial Redress Act.
[lxi]"Foreign Intelligence Surveillance Act of 1978, enacted on 25 October 1978, Pub. L. 95-511; Electronic Communications Privacy Act of 1986, enacted on 21 October 1986, Pub. L. 99-508; Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act Of 2001, enacted on 26 October 2001, Pub. L. 107-56."
[lxii]Andreas Wiebe& Nils Dietrich, Open Data Protection - Study on legal barriers to open data sharing - Data Protection and PSI (2017).
[lxiii]Jack Hyland, *Data Protection in EU Businesses: an Introduction to GDPR*, 1 DBS Business Review 146-148 (2017).
[lxiv]Klayman v. Obama, United States Court of Appeals, District of Columbia Circuit.
[lxv]Marina ŠkrinjarVidović, *Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities*, 11 Croatian Yearbook of European Law and Policy (2015).
[lxvi] Constitution of India, Article 19 (1950).
[lxvii] Constitution of India, Article 21 (1950).
[lxviii]Govind v. State of M.P., AIR 1975 SC 1378.
[lxix]Rowena Rogues &Vagelis Papakonstantinou, Privacy and data protection seals.
[lxx]Apar Gupta, Commentary on Information Technology Act, 269 (Lexis Nexis, 2013).
[lxxi]Kamlesh Bajaj, *Promoting Data Protection Standards through Contracts: The Case of the Data Security Council of India*, 29 Review of Policy Research 131-139 (2012).
[lxxii]Sreenidhi Srinivasan and Namrata Mukherjee, *Building an Effective Data Protection Regime*', Vidhi Centre For Legal Policy (2017).
[lxxiii]A. Wankhede, *Data Protection in India and the EU:* 2 European Data Protection Law Review 70-79 (2016).
[lxxiv] "The definition of terms "wrongful gain" or "wrongful loss" is not mentioned under the IT Act, reliance may be placed on Section 23, IPC which states as follows:
—"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

"Wrongful loss".—"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.‖ "

[lxxv] "Section 43 A of the IT Act states that the "reasonable security practices and procedures" can either be come into consensus between the parties or according to the specified law, and if the above mentioned doesn't exist that the practices adopted by the central government shall be adhered to"

[lxxvi] "It is pertinent to remember that if any person without the permission of the owner or any other person who is in charge of the same, attempts or assist someone else to make a copy of the information provided by the data subject shall be liable under section 47 of the IT Act to pay damages to the person so affected"

[lxxvii]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 5 (2011).

[lxxviii] Ibid

[lxxix] Ibid

[lxxx] Ibid

[lxxxi] Ibid

[lxxxii] Vidhi Agarwal, *Privacy and data protection laws in India*, 5 International Journal of Liability and Scientific Enquiry 205 (2012).

[lxxxiii]Dr. Ajay Kumar Garg & Shikha Kuchhal, *Data Protection Laws in India: A Comparative Study*, 3 Indian Journal of Applied Research 75-76 (2011).

[lxxxiv] Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits*' 2 ,Kluwer Law International (2002).

[lxxxv] Jerry Kang, *Information Privacy in Cyberspace Transaction*s ', 50 Stanford Law Review 1193, 1202-03 (1998).

[lxxxvi]Erne Mraznica, *GDPR: A new challenge for personal data protection*, 46 Bankarstvo 166-177 (2017).

[lxxxvii]P. T. J. Wolters, *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, 7 International Data Privacy Law 165-178 (2017).

[lxxxviii] "By asking for consent, the data subject is responsible for managing her/his own information, thereby leading to "privacy self-management", which originated in the Fair Information Practices (FIPPs), created in the 1970s in order to address concerns about the rising digitisation of data.' Daniel Solove, *Privacy Self-management and the Consent Dilemm*', 126 Harvard Law Review (2013).

[lxxxix] Maria Tzanou, *Data protection as a fundamental right next to privacy? _Reconstructing' a not so new right*,' 88 International Data Privacy Law (2013).

[xc]Sandeep Mittal I.P.S., *Old Wine with a New Label: Rights of Data Subjects Under GDPR*, SSRN Electronic Journal (2017).

[xci]Paul Voigt & Axel von dem Bussche, The EU general data protection regulation (GDPR) (2017).

[xcii] [In Indian Legislations per day civil penalty that may be leviable is capped to an upper limit. For instance Companies Act, 2013 under Sec. 91(2) provides that civil penalty for closure of register of members or debenture holders without prescribed notice is Rs. 5,000 for every day of such violation subject to a maximum of Rs. 1 lakh. Although, the IT Act, has examples, like, Section 44(b) which prescribes a per day civil penalty of Rs. 5,000 which is not capped.] Srikrishna, B., et. al. (2018). White paper of the committee of experts on a data protection framework for India. [online] Available at: http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited [Accessed 4 Aug. 2018].

[xciii] [For instance, per Section 105, Insurance Act, 1938, under Sec. 105 states if any director, managing director, manager or other officer or employee of an insurer wrongfully obtains possession of any property or wrongfully applies to any purposes of the said Act, then such person shall be liable to a penalty not exceeding Rs. 1 crore. Further, per Section 50, Food Safety and Standards Act, 2006, any person who sells to the purchaser's prejudice any food which is not in compliance with the provisions of the FSSA or of the nature, substance or quality demanded by the purchaser shall be liable to a penalty not exceeding Rs. 5 lakhs.] Ibid 92

[xciv] [For example SEBI Act under Sec. 15G, penalizes insider trading with minimum of Rs. 10 lakhs which may extend to Rs. 25 crores or three times the amounts of profit made out of insider trading, whichever is higher. Similarly, under Section 27, Competition Act, 2002, where after any enquiry, it is found that any agreement or action of an enterprise in a dominant position is in contravention of Sections 3 or 4, as the case may be, a penalty may be imposed which shall not be more than 10% of the average of the turnover for the last three preceding financial years upon each of such person or enterprise which are parties to such agreement or abuse.] Ibid 92

[xcv]The Finance Act amended the IT Act to confer the jurisdiction of the CyAT on the TDSAT, in order to bring harmony, uniformity and efficiency in the appeal hearing process. Although the efficiency of the TDSAT to hear the matter of CyAT with its existing burden is matter of worrisome.

[xcvi]Anupam Chander in his article entitled "Data Nationalism" draws a picture where the data stops for a check post at the boundary of the nation so as to see whether data shall stay or cross the boundaries., along with its probability for taxation. He states that while it may sound fanciful, this would be the ned effect of the policies that are being adopted worldwide to restrict the flow of data outside the national boundaries..

[xcvii]Julian Wagner, *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?*, International Data Privacy Law (2018).

[xcviii] GDPR through its Article 45 states an adequacy test for transfer of personal data to a third country, which stipulates that transfer of personal data of EU subjects to non- EEA countries is prohibited unless they meet the criteria set by the tests.

[xcix]Article 93(2), EU GDPR.

[c]*Ibid*

[ci] The EC has the authority to determine that certain standard contractual clauses offer adequate protection with regards to data protection while undertaking transfer of data to non-EU/EEA countries

[cii] The data transfer that takes place under their contract are implied to have immunity under the GDPR regime. Considering the difficulty encountered by the stakeholders to comply with the set standard to safeguards, alternatives like that of model contract clauses would play a leading role in facilitating the transfer of data in any member states.

[ciii] "The surveys have found out that the companies established in the jurisdictions with forced data localization requires 30-60% more for their computing needs against the opportunity to take data outside country borders\" Erica Fraser, *Data Localisation and the Balkanisation of the Internet'*, Scripted 359 (2016).

[civ] "The data localization may prove helpful in safeguarding the rights of subjects in certain circumstances, though the cons weigh against the cons"

[cv] "The data localization may help reduce foreign surveillance, but would effectively increase the risk of local surveillance by law enforcement agencies."

[cvi]'"an example of the same would be the Microsoft case where the extra territorial application of the US's Stored Communications Act was denied and the applicability was restricted to data store locally.For instance in the Microsoft case, it was held that US's Stored Communications Act cannot be applied extraterritorially, and can only be applied to data which is actually stored in the country."'

[cvii] "A negative impact of the data localization has been witnessed in several countries (Brazil -0.8%, India -0.8% and Republic of Korea -1.1%) or implemented (Indonesia -0.7%)." UNCTAD, Data Protection Regulations and International Data Flows: Implications for Trade and Developments (2016),