DATA PROTECTION IN INDIA: PRIVACY, PERSONAL DATA, AND THE SAGA OF A LEGISLATIVE AND ECONOMICAL APPROACH

Acharaj Kaur Tuteja[1] *and Digvijay Singh*[2]

ABSTRACT

Set to become the most populated country, India has always lacked an adequate legal framework for protecting the data privacy of its citizens. While random attempts have been sprung at the Parliament from time to time, there still remains an astonishing lacuna in that aspect. The same has been tried to bridge through the recent Data Protection Bill, 2022 with its 30 clauses articulated for the supposed benefit of data principals. The following research paper, takes the assistance of secondary research to delve into the economic analysis of the Bill and how it strategically contradicts the purpose and objective of its creation that is – data privacy protection. Through adoption of Coase theorem and game theory, this paper seeks to elaborate on the provisions of the Bill and how they lack an appropriate economic trade-off for most individuals involved. Right to privacy was deemed a fundamental right in 2017 itself, and the project outlines the disruption of this Apex Court judgement from an economic point of view.

Keywords: *Right to Privacy, Data Protection, Sri Krishna Committee, Coase theorem, game theory, costs and incentives*

[1] Author is a 4th year student at the Gujarat National Law University.
[2] Author is a 4th year student at the Gujarat National Law University.

1. HYPOTHESIS

Following the theme of the research, we can derive a variety of factors keeping in mind the interplay of law with economics; it was observed that privacy is nuanced and citizens desire more privacy; hence when there is backing and legislation for more privacy, the consumer respond leading to increased confidence and increased economic efficiency hence it can be said that increased privacy leads to increased confidence leading to increased efficiency.

We can also see that this has negative connotations, as we noticed from the analysis of the Coase theorem that the transaction costs here are not zero; this impacts the total costs as the power to negotiate between the parties is not equal.

The analysis of the data protection bill, it can be derived that the powers equation and balance is not really at an equal position. Hence, this gives the state a higher bargaining power and decisionmaking power, giving it more leverage and authority. Hence, the state has the propensity to expand on it economically.

We have also analyzed the breach of data, privacy, and data protection tool from various economic tools, we also look at the constitutional aspects of economics of privacy in detail.

1.1 Research Methodology and Objectives

This paper adopts an exploratory research approach to investigate the necessary information from various secondary sources, such as published research works, RBI reports, and government reports, along with constitutional precedents and approaches.

We looked at the legislative framework provided in our constitution on privacy and the precedents looked at the Supreme Court to understand the jurisprudence that exists in India; we also looked at the various approaches that other nations have taken and the perception people have about privacy. We then contrasted the same with the various theories of economics like the game theory and its interplay with privacy, cost-benefit analysis of data, Coase theorem and analysis of economic surveys done. We also approached data from the perspective of positive externalities.

Eventually, we looked at the draft of the data protection bill and how it would have its own economic nuances and effects and how it would have a role to play when analysed from an

economic perspective.

Looking at the objectives of the study, the implementation of the Personal Data Protection Act of 2023 marks a significant milestone in data governance, introducing stringent regulations governing the collection, processing, and storage of personal data. With a focus on enhancing privacy rights and empowering consumer choices, the legislation compels businesses to adopt more transparent and ethical approaches to data management. This shift not only fosters greater trust and accountability in the digital landscape but also stimulates innovation and competition within the marketplace.

As companies adapt to comply with the provisions of the new law, they are compelled to recalibrate their business models to accommodate evolving consumer preferences and privacy concerns. By prioritizing data security, transparency, and user consent, businesses can cultivate stronger relationships with their customer base, fostering loyalty and bolstering brand reputation. The enactment of stringent data protection regulations not only stimulates economic growth but also drives sustainable development, paving the way for a more privacy-centric and consumer-friendly digital ecosystem in the long term.

2. INTRODUCTION

When referring to data privacy, the landmark judgement of *Justice KS Puttaswamy v. Union of India*[3] leaves little to interpretation. It continues to be the pedestal for "Right to Privacy" being recognized as a fundamental right in the country of India. A nine-judge bench, the decision allowed for inclusion of right to privacy as an overarch of right to life at large and guaranteed under Part III of the Constitution.

The facts of the case involved a petition being filed by the aforementioned retired judge of Karnataka High Court, in regards to the Aadhar Project initiated by the Unique Identification Authority of India (UIDAI). UIDAI claims that, "Not only it is a fool-proof method of identifying a person, it is also an instrument whereby a person can enter into any transaction without needing any other document in support. It has become a symbol of digital economy and has enabled

[3] Justice KS Puttaswamy v. Union of India, (2017) 10 SCC 1.

multiple avenues for a common man." A 12-digit Aadhar number was to be given to every Indian citizen. The government wished to make a uniform biometrics-based identity card mandatory for accessing public schemes and benefits. Judge KS Puttaswamy challenged the validity of the same saying that it violated the right of privacy. The standards for the collection of demographic biometric data by the government were contested in 2015 before a three-judge bench of the court on the grounds that they violated the right to privacy. Based on the rulings in *M.P. Sharma v. Satish Chandra*[4] and *Kharak Singh v. State of Uttar Pradesh*[5], the Attorney General of India argued against the existence of a fundamental right to privacy. The three-judge bench took note of recent Supreme Court cases where the right to privacy had been declared to be a fundamental right that was protected by the constitution while examining these issues. However, the benches in all those cases that reaffirmed right to privacy as a fundamental right, constituted a lesser strength than the two cases cited by the Attorney General.

The Supreme Court, pronounced privacy to be a distinct and independent fundamental right under Article 21 of the Constitution. The decision's core outlined a broad understanding of the right to privacy, one that included decisions, choices, information, and freedom rather than being restricted to physical invasion or a derivative right under Article 21. It was determined that Part III of the Constitution's fundamental right to privacy was both enforceable and comprehensive. The several opinions included specifics pertaining to the right's scope.

"The right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails."

Subsequently, the government set up a Parliamentary Committee under the chairmanship of Justice BN Srikrishna that advanced a report alongside a draft data protection bill in 2018. The Committee noted that the legal framework must strike a balance between the interests of the individual with regard to his personal information and those of the organization, such as a service provider, that has access to this information. It was said that the connection between the client and the service provider ought to be seen as a fiduciary one. This is brought on by the person's

[4] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[5] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

reliance on the service provider in order to acquire a service. As a result, the service provider handling the data has a responsibility to treat the individual's personal information fairly and to use it only for those reasons that have been approved. The same was struck down and a much more controversial version of it emerged in the following year. The Personal Data Protection Bill, 2019 was presented to the Committee that gave its report and a new draft in 2021. The same was rejected by the Centre on grounds of it having extensive and unacceptable changes, making this the fourth attempt at introducing a legal framework and protecting personal data.

The Ministry of Electronics and Information Technology, on November 18, 2022, introduced the Digital Personal Data Bill, 2022. If passed, it is set to fill the lacunae present in the current IT SPDI (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules notified in 2011. The bill seeks to regulate and place obligations on Data Fiduciaries (any person who alone or along with other persons determine purposes and means of processing) and Data Processors (personal who processes personal data on behalf of a data fiduciary). The data fiduciary, under this proposed law, is required to provide an itemised notice in clear and plain language containing a description of the personal data needed and the purpose for which such data has been processed, as soon as it is reasonably practicable to the data principal. The factor of consent has been given considerable importance. According to the provisions, notice can be "a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed."

Dissection of the Bill provides us with the rights and duties of the Data Principals (individuals to whom the personal data belongs) enclosed in Chapter 3. It ranges from the right to information regarding their personal data being processed by companies, right to withdraw consent for their data to be processed once they know relevant details of the same or even the direct right to request erasure of incorrect and incomplete information. For example, data taken for an e-commerce delivery can be eradicated from the system once delivery is made. Next, the right to approach the appropriate authority appointed by the company in case of a grievance the contact details of a Data Protection Officer must be published and easily accessible. A Data Protection Board would exist for appealing the decision within seven days. Additionally, there exists a right to nominate another individual for carrying out their rights in case of death or incapacity.

3. CONSTITUTIONAL DILEMMA OF THE STATE BREACHING PRIVACY

According to Article 21 of the Indian Constitution, the right to privacy, which is itself protected by the right to life and personal liberty, includes the right to be forgotten. As stated before, the judgement of Justice K.S. Puttaswamy v. Union of India, ruled privacy to be a natural right that is necessary to lead a decent existence, the right to privacy has been incorporated into Article 21. Everyone has the right to protection from anyone attempting to violate their privacy without a good reason or legal justification. Naturally, the person should also have a right to this information if it has been made available to the public or to any third party.

The Data Protection Bill, 2022 however brings in the factor of information that is pertinent to the public or national security. It allows the Central Government, under Section 18, to exempt certain data from privacy protection – "by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these." The Bill even seeks to amend the Right to Information Act, 2005 under Clause 30(2). Section 8(1)(j) of the

RTI Act is an exception. It states that –

"(j) information which relates to personal information the disclosure of which has not relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information: Provided that the information, which cannot be denied to the Parliament or a State Legislature shall not be denied to any person."

Given the lack of adequate surveillance laws in the country, this places an abnormal amount of power in the State's hand which in turn is a threat to right to privacy. The Indian government will have access to information on a scale never before possible in conjunction with the localization requirement for data. The Bill will become an excuse for them to exercise authority blindly since there is no third-party check, no need for informing the surveillance subject or even introduction of court orders. To top this on the proposal of an outside committee, the draft bill grants the central

government the right to nominate members of the data protection authority. Five years seems like a very little time to allow a new institution the chance to get its feet under it and achieve the independence it needs to function as a regulator. For reasons outlined in the legislation, the central government may also dismiss members of the authority.

The immense regulation power that has very strategically been given up to the Government, will economically affect the market. For market exchanges, regulation results in a social transaction cost that is shared by the general public and the parties involved. In some cases, the expense of the rule might outweigh the net efficiency improvements it brings about. More regulation has diminishing returns in the same way that it does for producers and consumers, and eventually it becomes too expensive. Application of the Coase theorem would suggest, that such a situation involves higher transactional costs which leads to less scope for bargaining for consumers and in turn an inefficient outcome.

4. ECONOMICS OF NON-COMPLIANCE AND BREACH OF PRIVACY

Privacy as a concept has been somewhat difficult to fit into watertight compartments. While most people hold it synonymous to mere concealment of information, it sometimes goes beyond that to autonomy and personal freedom.[6] And of course, economists have taken a particular interest in that aspect. They focus on the line that separates information kept to self and that released and put forth to the public. This in turn revolves around the trade-off between protecting or sharing personal data. The Data Protection Bill, 2022 defined personal data as "any data about an individual who is identifiable by or in relation to such data." The massive strides that information technology has made in recent years, has increased the amount of individual information that can be collected and stored for various purposes. This has inherently led to open access to a person's details such as their income, address, gender, and age by third parties usually without actual consent. These are then religiously studied as business tactics for advertising and target services.[7]

[6] Richard A. Posner, *The Economics of Privacy,* 2 THE AMERICAN ECONOMIC REVIEW 71, (1981), http://www.jstor.org/stable/1815754.

[7] David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy,* 3 THE JOURNAL OF ECONOMIC PERSPECTIVES 23, (2009), http://www.jstor.org/stable/27740539.

Data holders are have clearly benefitted from the same, but the rising concern amongst internet users about their personal data privacy cannot be ignored.

The issue that remains is the divide that comes from information asymmetry. Take an example of a seller who has access to how little you know about a certain product he is selling, the same can be used to exploit you. Alternatively, a real-estate company might hire the wrong employee due to a lack of personal data available. The society or an individual may equally benefit from certain information either being suppressed or revealed. Further, the cost of protecting their data might be dependent on how much others are revealing about themselves (for example, various online blogs require you to compulsorily have a social media id in order to gain access to their articles) or just impossible completely since the websites can analyse their data on the basis of what similar people had to say about their interests.[8] While firms are actively engaged in this personal data exchange market, the individual has little to no awareness of this chain and in turn, less opportunities to curb the flow.

The Bill through its concept of notice and consent tries to place greater autonomy in the hands of the individuals. Section 25, in regards to non-compliance and breach of privacy, states that –

"If the Board determines on conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crore in each instance."

Now, the Bill proposes a penalty of up to Rs. 250 crores if the data fiduciaries fail to provide reasonable safeguards or inform the Board in cases of the personal data breach. The question here is whether the determination of the penalty has been done proportional to the consumer harm, which is difficult to measure alongside the amount of liability that these firms may have. Setting the punishment at a higher level, obstructs innovation and doing it at a lower level will legitimize the intrusive behaviour, making the fiduciaries believe that it is just a production cost that they need to incur. The Bill places absolute liability on the data processors and the data fiduciaries without considering their intent in having done so, causing a disproportionate burden. This creates a certain level of inefficiency since firms more vulnerable to data breaches are placed on an

[8] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 2 JOURNAL OF ECONOMIC LITERATURE 54, (2016), http://www.jstor.org/stable/43966740.

uneven footing with other organizations.

Delving into the costs of protecting data reveals that in two ways, protecting customer data may be expensive for firms. First, in order to save future privacy costs, businesses can postpone potentially profitable data collection, mining, and processing. In terms of economics, this represents an opportunity cost. Second, companies may spend lesser but specific ex-ante expenditures in an effort to avert ex-post projected losses brought on by privacy scandals by aggravated consumers. Businesses may elect to invest in data security and protection, sometimes overinvesting. Additional costs comprise the social losses due to incoherent privacy policies amidst a complex array of legislative and self-regulatory initiatives, both consumers and firms are uncertain about the level of protection afforded to, or required for, various types of personal data. This uncertainty is costly in itself, in that it forces data subjects and data holders to invest resources into learning about the admissibility of a given data practice.

However, these costs might attract consumers who are intent on protecting personal information and end up developing a sense of loyalty towards these firms that are dedicated towards data privacy. By limiting liabilities of misused data, the firms can ensure a set of customers who regard privacy at a higher pedestal than most. Thereby, equating the cost of data security and protection to the benefit of an increased revenue being earned.

5. ECONOMICS BEHIND COSTS INCURRED

Privacy has always been considered as an aspect that deals with individual liberty, freedom, and morality. It has been an accepted norm throughout the globe that an individual must be given right to keep their private information to themselves and should be provided the ability to choose whether they wish to impart such information or not. Across the globe, there are legal texts and laws with legislative mandates which imply this, and in the absence of such legislation, there are always laws which imply a right to privacy. Like in India, the constitution came in effect in 1950 and had no mention of right to privacy but it was through the gradual process of time, the right to privacy was interpreted to be applied and the genesis was found in article 21 of our constitution. There has been a paradigm shift in the thinking as privacy today is not just a concept to be

deliberated under public policy but a concept which is also being deliberated under economics[9] Similarly, there has been minimal mention and analysis of privacy as an economic concept but with the process of time and the rise of data analysis to interpret market patters, we see this emerging aspect where privacy has been looked through an economic perspective where there is an overview of an individual's privacy through the cost and value of his data and credentials. This usage of personal data comes at a cost.[10]

In this changing environment of data and digital technology, today, we see that a lot of companies, firms and service providers request data from individuals while signing up and at the time of providing such service, one of the primary objectives of such data collection is an accumulation of information attached and associated with such a person and then using such attributes for the purpose of sales of various good and services. This leads to costs being attached to such product and service and this also leads to such service or product being competitive, the firm with more information would make more sale and this at time would come at the cost of privacy of the person imparting that information, as there is not only a lack of jurisprudence currently but there is no guiding law which decides or provides a background to deal with such economic costs of privacy. One of the concerns also remains is the factor of consent as there is enough evidence to prove that the consent of such a person is taken before using their information for commercial purposes. While this may be one of the aspects behind the economics of privacy, there are other aspects to privacy as well.

We must look at the market costs of privacy before we can examine the effects of privacy economically. The connotations can either be positive or negative. Take the labour market as an example. A job seeker who bluffs (or withholds information from the company) could hurt his chances of landing the position. This results in a negative cost because by hiding the knowledge, the seller (labour) lowers the market's efficiency because the buyer (employers) would be unable to meet expectations. Contrarily, if an employee withholds knowledge that could propel him to a higher position, it will cost the company money because he won't be able to operate as efficiently

[9] KS Puttaswamy & Anr. v. Union of India and Others, (2017) 10 SCC 1.

[10] Smith, R., Morrow, R., & Ross, *Intervention Costing and Economic Analysis*, 3 IN FIELD TRIALS OF HEALTH INTERVENTIONS 18, (2015), https://med.libretexts.org/Bookshelves/Nursing/Field_Trials_of_Health_Interventions__A_Toolbox_(Smith_Morrow_and_Ross)/19%3A_Intervention_costing_and_economic_analysis/19.02%3A_Types_of_economic_analyses.

as the market, hence here the key factor is the transmission of Information in a perfect market, where there would be same access of knowledge to all the players, privacy would be low as there would be less concealment of any information. Such view was also endorsed by Richard Posner when he said that the protection of privacy creates inefficiencies in the marketplace, since it conceals potentially relevant information from other economic agents

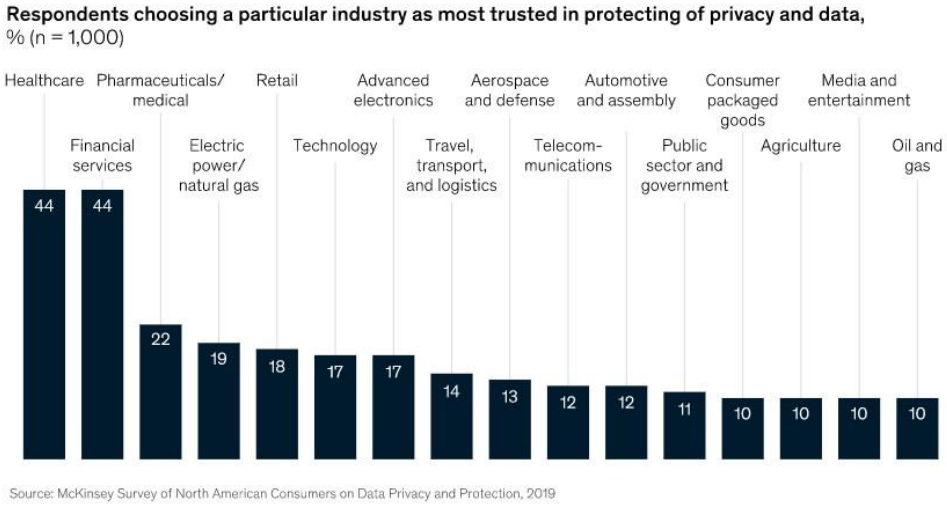
This occurs because a worker who withholds information raises the price of the good or service. As soon as the person starts working, the efficiency will drop when they are combined with the pool of qualified workers, raising the price of goods or services. Also, this will impact the market since rising prices for products and services will cause market inflation, which will eventually result in a decline in the average income level for the workforce. Moreover, if in the market a situation arises where most information or knowledge is withheld, the prices would remain uncertain as there would not be enough understanding to ensure that a price for such good can bet determined.

Privacy also needs to be seen as a tool for empowerment, as we understand that if there are adequate mechanisms to ensure that the state can protect the privacy of Individuals, the efficiency of those working in the markets would certainly increase as there would be more confidence in the market, and with consent, people would also not hesitate to share information with other people and firms if they are sure that their information is secured and the mechanism. This might be a new arena, but the economic cost of privacy is extremely relevant and crucial. This reasoning is the stepping stone behind the nuances of privacy in India.

6. DATA FROM A COST-BENEFIT ANALYSIS

It is important to look at data from a cost-benefit analysis, as there are certain tradeoffs which are involved here, first of them being would a rational consumer be willing to part ways from their data while consuming a product, what would be the cost of such action and will the incentive which is derived from parting away from such data be enough to motivate the rational consumer from parting away from his data, in various studies and events it is understood that there would in very few cases a consumer be willing to part ways with their data as personal information and privacy in an nuanced positions are considered to be sacrosanct, despite the benefits , this was

also concluded in a study done by McKinsey and Co. [11] this happens because a consumer understands that in any scenario the benefit should always be higher than the value of privacy in such matter, that is why in the McKinsey report it is noticed that a consumer would be willing to share its data with the government to derive incentive from the government and they see the benefit and since it is the government the level of trust is also high and the consumer would not feel that their data is misused



Moreover, it becomes more difficult to look at a cost-benefit analysis primarily because, the trust a rational consumer has also depended from firm to firm and sector to sector, so per data from My analyst firm McKinsey, a consumer would be more willing to share their data with a hospital than with a fashion company because of the type of industry and the cost-benefit analysis that they see in them.

We can also understand this with the example of the simple app called LinkedIn, where people voluntarily upload their personal information primarily because it connects them with other people who desire such attributes from the person and this certainly creates an atmosphere where the person is incentivized to upload their data as the benefit is higher than the cost even if the data which is personal comes in the public arena

[11] Jacques Bughin, and Jonathan Godsall, *The Consumer Data Opportunity and The Privacy Imperative*, McKinsey & Company, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumerdata-opportunity-and-the-privacy-imperative.

7. AN ECONOMIC ANALYSIS OF DATA LEGISLATION

To "process the digital personal data of the individuals respecting their rights and balancing the requirement to process the personal data legitimately," the Digital Personal Data Protection Bill, 2022 was drafted. The Personal Data Protection Bill 2019, which was then being developed, was not codified, so this is the second attempt by the Indian parliament to enact a data protection law in the nation.

It must be kept in mind that any such legislation that comes to the fray in India would be a regulatory one which would require much more compliance so that might have a sweeping impact on businesses in India, and this would also be the reason variable costs of the companies would shoot up because of increased regulations and regulatory framework but as a value which is intrinsic to human life, ta middle ground needs to be found where the line can be drawn.

7.1 The Prism Of Coase Theorem

Let's us say that there exist two parties. The two parties in question can negotiate and find an effective solution if the transaction costs are low and property rights are properly established. For instance, the data subject might sell the data controller their personal information, or the controller could compensate the data subject for the use of their information as this would be a situation which would provide negotiating power to both parties to come at a situation where the most optimal option and can be decided.

But, in practice, the costs of drafting such an agreement could be substantial, particularly for individual data subjects who might not have the means or negotiation leverage. Furthermore, as the use of personal data frequently involves legal and moral considerations, the property rights over that data may not be clearly defined.[12]

The rational consumer receives the power to negotiate his position with the help of data and this in fact is a way they empower them with the power to negotiate, Coase in fact has a view on this himself where he argued that In the case of privacy, Coase's Theorem suggests that control over data will go to the party that values it the most, regardless of who initially has the "right" to the

[12] RH Coase, *The problem of social cost. Journal of Law and Economics*, (1960).

data (i.e., whether the individual must opt in or opt out).[13]

But when it comes to transaction costs, Coase's theorem requires transaction costs to be near zero for parties or at a stage where in the longer run they are irrelevant so that they are not a factor which either allow negotiating power to either of the parties and also to and the end result to negotiate an efficient outcome. However, the transaction costs of privacy decisions can be significant, especially when consumers must opt in for companies to be able to use the data. Obtaining affirmative consent imposes significant costs on businesses as there is increased vigilance and a sense of security when it comes to data.

7.2 A Prism of Game Theory

Game theory is one of the tools we can employ to understand the nuances of privacy from an economic perspective, let us take a data subject and a data collector, such as a social networking site or an advertising network (such as an individual consumer). The decision to acquire or not to collect personal information from the data subject is up to the data collector, and the decision to provide personal information is up to the data subject and this can also be a variable as there ia high chance that when such a collector is the government in. the game theory, the perceived level of trust would be high so in a model of game theory, a rational consumer is likely to take a chance an act on it. What game theory here would essentially do is provide stricter privacy regulations or increased transparency requirements may change the beliefs and preferences of the players, leading to different equilibria. In addition, the game can be extended to include multiple data collectors and multiple data subjects, as well as other parties such as regulators or advocacy groups. Overall, game theory provides a powerful framework for analyzing the strategic interactions between individuals and firms in the context of data protection and privacy.

This model's main presumption is that the data collector only has partial knowledge of the preferences and traits of the data subject. It is possible that the data subject has privacy preferences that the data collector is unaware of or that the subject has security concerns about their personal information that the data collector is unable to see.

The game can be seen as a matrix, with the rewards for the data subject and the data collector

[13] Information Technology and Innovation Foundation, *The Economics of Opt-Out Versus Opt-In Privacy Rules* (6 October 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/.

based on their individual decisions. As an illustration, if the data collector gathers personal information from the data subject and uses it for targeted advertising or other reasons, the data collector may profit from doing so, and the data subject may profit from using the platform or service that the data collector offers. Yet, if the data collector gathers personal information and the data subject chooses not to disclose it, the data collector may still be responsible for the costs of data management and storage while the data subject is left out of the picture. The game can have multiple equilibria, depending on the preferences and beliefs of the players. For example, if the data collector believes that the data subject is privacy-sensitive and the data subject believes that the data collector will not use their personal data ethically, the game may result in a lowinformation equilibrium, where the data collector does not collect personal data and the data subject does not provide it. On the other hand, if the data collector believes that the data subject is not privacy-sensitive and the data subject believes that the data collector will use their personal data ethically, the game may result in a high-information equilibrium, where the data collector collects personal data and the data subject provides it.

Game theory essentially pans out the usage of data and privacy in a model which depends on situations and players to achieve an outcome that is the most probable [14]

8. POSITIVE EXTERNALITY OF PERSONAL DATA

There are several instances like this one where there are social benefits when data is shared, and citizens go beyond the nuances of privacy; this perhaps happens because there are several citizens out there who, let us say, share their health and medical data allowing to map more data and create patterns to study diseases. Still, on the same hand such profiling only leads to situations where an economic public good is created which is in the larger benefit of society.

Similarly, where data about the position of cars and traffic is shared, the outcome is more efficient as more citizens can manage traffic better, allowing a positive externality and creating public incentives to share data, but there needs to be proper analysis as to where the line can be drawn between a public good which creates economic incentive for all and the problem of free rider.[15]

[14] George Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEG. STUD. 623 (1980).

[15] Lacker, J. M., & Weinberg, J. A., *The economics of financial privacy: To opt out or to opt in?,* JOURNAL OF MONETARY ECONOMICS (2007).

9. THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022: AN ECONOMIC PERSPECTIVE

This discussion stems from the usage of personal data, it is defined as Personal Data according to The Digital Personal Data Protection Bill, 2022 is defined as "data about an individual which is identifiable". We find similar definition of personal data under General Data Protection Regulation (GDPR) which states that "personal data are any information which are related to an identifiable or identifiable natural person." Further, under the European Union Data Protection Regulation Directives adopted in 1995 provides for the definition of personal data as "any information relating to an identified or identifiable natural person; an identifiable person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological or mental and other attributes in the genre, economic and financial, cultural or social identity of a person. Personal data can provide a basis which could lead to profiling of such a person and drawing and economic incentives out of the same.

There has been a lot of deliberation on the need for a new bill which is promptly required to take care of privacy needs but under the absence of such legislation, the current legislation is the Information Technology act of 2000. The legislation covered data breaches, and data privacy, and it set out the penalties for those who violate data privacy and commit other offences relating to cyberspace. The act contains a few significant parts that deal with personal data. Section 43 of the Information Technology Act of 2000 is the most significant; it states that if any person uses a computer, computer system, or computer network without the owner's or another person in charge of those devices' permission, that person shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. While the act has several provisions to deal with such notions of privacy, the act has several lacunas which need to be fulfilled, especially considering the time gap that has been existing.

The contention over who owns the personal data is what gives it its commercial value. Who owns the data of an individual? is the key issue that captures the entire discussion. Because of this ownership, personal data is now commercially viable. Corporations are the only entity holding the financial worth of personal data. The fact that these businesses approach personal information as a commodity transforms it into a resource. Given the scarcity of this resource, figuring out who

owns it is crucial to estimating its economic worth. When addressing this question in a particular jurisdiction, it facilitates a more complex use of personal data.

There are experts and analysts who today argue that while this might be the situation now, in the absence of a proper data regime, things will only get worse in the future as with the advent of Artificial intelligence, the data that we consume could be segregated more properly, reducing the economic costs for the same, with the such advent of data there would also be serious concerns, like highlighted by Thomas Piketty as he argues that this might lead to economic inequalities as there would be differentiation in how such data is being collected and perceived. There would be institutions and organisations who are better equipped to deal with the collection of such data who would certainly incentivize of such data, while others would not. There are probable scenarios where some corporates and institutions would gather such information and capitalize on it this would also lead to ensuring that the capabilities and resources of firms which are smaller are not able to match the talent and technology of firms which have more manpower, resources [16]

Thomas Piketty also highlighted that various nations around the world have brought in legislations to ensure that data protection is given a priority, this is certainly a measure of economics ac=long with being a step for public policy as this ensures that there is a sense of semblance and parity while allocation of resources which in this case is data. This emphasis on data is certainly useful to ensure that we today understand the nuances of data protection.

Now, the data protection bill would have its own nuances and would certainly be step in the right direction as it has economic consequences as it would make the data more valuable calling for increase of demand for such data and more stringent action by la from the government

The contention over data ownership is what gives personal data its economic value. The question "who owns the data of an individual?" can be used to summarize the entire discussion. This ownership is what makes personal data economically valuable in the market. Corporations are the only entity holding the personal data's economic value. Personal data is a resource because these businesses regard it like a commodity and handle it as such. Due to this resource's scarcity, determining who owns it and how much it is worth to the economy is crucial. When the answer to this question is provided in any jurisdiction, it facilitates a more complex use of personal data.

[16] Tomas Piketty, *Tomas Piketty: Big Data Limitations,* (2014), https://www.weforum.org/agenda/2014/05/tomas-piketty-big-data-limitations/.

While corporates and firms are one of the major players who desire to possess data of consumers, the government is also another data which possesses data and it as a body cannot be entrusted with data as well; there need to be protection as well as to how the government of a nation can harvest and use such data, as pointed out by economist and thinker Ruchir Sharma, data is dynamic in nature and governments through their record have the economic propensity to collect data of funds and assets of companies as well as individuals . This can often lead to policy making which deals with macroeconomic policy being made keeping consumers' data.

This demonstrates the legal status of personal data and its expanding economic significance, which draw our attention to a crucial idea without which any discussion of personal data would fall short—namely, privacy. Without an economic analysis of privacy, any discussion of the economic value of personal data would fall short.

10. CONCLUSION

In the modern era of data proliferation, safeguarding personal information and privacy has become paramount. Data protection is not merely a theoretical concept but a fundamental necessity in contemporary society, where the exploitation of data for selfish and financial gains poses significant threats to individuals and societies at large. The responsibility of ensuring data protection primarily lies with the state, which must enact robust legislation and regulatory frameworks to mitigate the risks associated with data misuse and abuse

At the heart of the discourse on data protection lies the understanding and definition of personal data and privacy. Without a clear understanding of these concepts, it is challenging to grasp the full implications of data protection measures. Privacy, in particular, is of utmost importance in the digital age, where individuals share vast amounts of personal information online, often without fully comprehending the potential consequences.

In the context of India, the judiciary's role in delineating and safeguarding privacy rights has been pivotal. The landmark KS Puttaswamy decision, which recognized the right to privacy as a fundamental right under the Indian Constitution, marked a significant milestone in the country's legal landscape. Through its deliberations, the judiciary elucidated various facets of privacy and its significance in the digital realm, laying the groundwork for a more nuanced understanding of privacy rights in India.

One critical aspect highlighted by the Puttaswamy decision is the consideration of privacy costs in legislative processes. Despite the judiciary's emphasis on the importance of privacy, there remains a glaring gap between legal discourse and legislative action. The failure of parliament to adequately account for privacy costs when crafting laws undermines the protection of individuals' privacy rights and exposes them to potential abuses of their personal data.

The disconnect between legal principles and legislative enactments underscores the urgent need for a more comprehensive approach to data protection in India. Parliament must actively engage with the principles elucidated by the judiciary and integrate them into legislative frameworks governing data privacy and protection. Moreover, stakeholders across sectors must collaborate to develop robust mechanisms for enforcing data protection laws and holding violators accountable.

In conclusion, the debate over data protection and privacy rights is not merely academic but holds profound implications for individuals, society, and the integrity of democratic institutions. Strengthening the legal and regulatory framework surrounding data protection is imperative to safeguarding individual liberties and fostering trust in the digital ecosystem. Only through concerted efforts and a steadfast commitment to upholding privacy rights can India navigate the complexities of the digital age while ensuring the dignity and autonomy of its citizens.